SCADAPack E Security
Technical Reference

Documentation

Table of Contents

Part I Security Technical 4

1 Technical Support ... 4

2 Safety Information ... 5

3 References ... 7

4 Terminology ... 9

5 Introduction ... 12

5.1 Standards ... 13

5.2 Operational Goals, Functionality Summary, & Standard RTU Operation ... 15

5.3 SCADAPack E RTU Security ... 17

5.3.1 What is DNP3 Secure Authentication? ... 18

5.3.2 How does DNP3 Secure Authentication Work? ... 18

5.3.3 What is AGA12? ... 20

5.3.4 How does AGA12 Work? ... 22

5.3.5 Supported AGA12-2 Functionality ... 22

5.3.6 How do DNP3 Secure Authentication and AGA12 Encryption Work together? ... 24

5.3.7 Highlights of SCADAPack E RTU Security ... 24

5.4 Licensing ... 27

5.5 Key Management ... 28

5.5.1 SCADAPack E Configurator Key Modes ... 29

5.5.2 Master Key Configuration ... 29

5.5.3 Compact Flash Entry and UTIL LED ... 31

5.5.4 Local USB Configuration ... 32

5.6 User-based Authentication ... 33

6 Telnet and FTP Authentication ... 33

7 Using SCADAPack E Security ... 33

7.1 Description of Security Facilities ... 35

7.2 DNP3 Secure Authentication ... 36

7.2.1 Challenged Functions ... 36

7.2.2 Security Settings ... 38

7.2.3 Aggressive Mode ... 41

7.2.4 Vulnerabilities Addressed ... 43

7.3 AGA12 Encryption ... 44

7.3.1 AGA12 Node RTU ... 45

7.3.2 AGA12 Gateway and Session Establishment ... 47

7.3.3 AGA12 Gateway RTU ... 49

7.3.3.1 Configuring an AGA12 Gateway RTU ... 51

7.3.4 Secure Communications and Node Operation ... 52

7.3.5 Typical System Layout ... 54

7.3.6 Addressing and Local Communication ... 55

7.3.7 Remote RTUs Communicating using an AGA12 Gateway ... 56

7.3.8 Operating as a Data Concentrator ... 57

7.3.9 Example Configurations ... 58

7.3.10 AGA12 Parameters ... 60

7.3.10.1 DNP3 Routing Table and AGA12 Settings ... 61

7.3.10.2 Fixed AGA12-2 Parameters ... 63
7.3.10.3 Vulnerabilities Addressed ... 64
7.4 DNP3 Routing ... 65
7.5 Peer Communication, Multiple Masters, & Start-Up and Shutdown ... 67
7.6 Security Considerations ... 68
8 Security Administration ... 69
8.1 Security File Management & Counterpart Entry Management ... 70
9 Diagnostics ... 70
9.1 DNP3 Secure Authentication Diagnostics ... 71
9.1.1 Diagnostic Example - No RTU Security Configured ... 71
9.1.2 Diagnostic Example - Incorrect Security Credentials ... 73
9.1.3 Diagnostic Example - Successful Critical Message Challenge ... 75
9.2 AGA12 Encryption Diagnostics ... 77
9.2.1 Diagnostic Filtering ... 77
9.2.2 Routing Rule Diagnostics ... 78
9.2.3 Diagnostic Example - Session Open Transactions ... 82
9.2.4 Diagnostic Example - Session Re-establishment Transactions ... 89
9.2.5 System Points ... 91
10 Attack Vectors & Requirements ... 92
10.1 Protocol and Configuration attacks on RTU ... 93
10.2 Routed Communication to RTU & Access to Gateway ... 95
10.3 RTU Local Port Access, Networked Configurator & Spoofing Master Address ... 96
10.4 IP Networked RTUs & Duplicated RTU Personality ... 97
11 Using AGA12 Security Components - Copyright ... 98

I Security Technical

©2013 Control Microsystems Inc.
All rights reserved.
Printed in Canada.

Version: 8.05.4

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

1 Technical Support

Support related to any part of this documentation can be directed to one of the following support centers.

Technical Support: The Americas

Available Monday to Friday 8:00am – 6:30pm Eastern Time

Toll free within North America	1-888-226-6876
Direct Worldwide	+1-613-591-1943
Email	TechnicalSupport@controlmicrosystems.com

Technical Support: Europe

Available Monday to Friday 8:30am – 5:30pm Central European Time

Direct Worldwide	+31 (71) 597-1655
Email	euro-support@controlmicrosystems.com

Technical Support: Asia

Available Monday to Friday 8:00am – 6:30pm Eastern Time (North America)

Direct Worldwide	+1-613-591-1943
Email	TechnicalSupport@controlmicrosystems.com

Technical Support: Australia

Inside Australia	1300 369 233
Email	au.help@schneider-electric.com

2 Safety Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

	The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.
	This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result** in death or serious injury.

⚠CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result** in minor or moderate injury.

CAUTION

CAUTION used without the safety alert symbol, indicates a potentially hazardous situation which, if not avoided, **can result in** equipment damage..

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and the installation, and has received safety training to recognize and avoid the hazards involved.

BEFORE YOU BEGIN

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠CAUTION

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.

• Remove tools, meters, and debris from equipment.
Failure to follow these instructions can result in injury or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and grounds, except those grounds installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove ground from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

OPERATION AND ADJUSTMENTS

The following precautions are from the NEMA Standards Publication ICS 7.1-1995 (English version prevails):

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.
- Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

3 References

- American Gas Association AGA12 Part 1 Recommendations (2006). See http://www.aga.org/our-issues/security/Documents/0603REPORT12.PDF
- AGA12-2 Protocol and Java Reference Application, see http://scadasafe.sourceforge.net/
- Distributed Network Protocol (DNP3), see http://www.dnp.org/

- IEC62351 Part 1 and Part 5 Standards (Available from IEC Webstore)

4 Terminology

SCADA Security and its options for Encryption and Authentication can be complex.

Refer to this glossary of terms used in this document. For additional definitions related to SCADAPack E, see *SCADAPack E Technical Overview*.

AGA12 Gateway RTU: An SCADAPack E RTU operating mode that performs encoding and decoding between cleartext 9 and ciphertext 9 on behalf of other nodes in the network. Commonly used to interface a secure AGA12 network to a cleartext master station. The DNP3 Host uses the AGA12 gateway feature of a SCADAPack ES to encypt plain text DNP3 messages frong from the Host to the RTUs in the field. The same gateway decrypts the cipher text messages coming back from the field RTUs to the Host.

AGA12 Node: A device providing SCADA Cryptographic Module (SCM) services in order to receive and transmit secure data to the AGA12-2 standard.

Authentication: A challenge and reply exchange between two devices that provides them both with confidence that the other device is who it claims to be.

Authority: An independent entity holding and providing security credentials. The SCADAPack E Security Administrator 11 application is an example of a simple authority.

Challenger: A device attempting to authenticate 9 that a partner device is who it claims to be. See also Responder 10.

Cipher Suite: A set of cryptographic algorithms, keys, and parameters identified by a cipher suite number. The AGA12 virtual SCM within each RTU maintains a mapping of every static session and every open dynamic session to a cipher suite (see also session 11)

Cipher text: Transmitted or received data that has been encoded (see also encoding 10)

Cipher text Port: In the context of SCADAPack E RTUs, this is a communications port supporting ciphertext DNP3. In the case of a AGA12 Gateway RTU, a ciphertext port may also support cleartext DNP3 when operating in mixed mode.

Clear Device Port: Applies to SCADAPack E AGA12 Gateway RTU only (see AGA12 Gateway 9). This port receives DNP3 data in cleartext and encodes it for transmission on a ciphertext port. A clear device port transmits cleartext DNP3 data after it has been decoded from reception on a ciphertext port.

Cleartext: Data that has not been encoded (see also encoding 10). It may be received data, that is to be transmitted 'in-the-clear,' data that is yet to be encoded, or data that is already decoded 9.

Common Key: A cryptographic key value that is used amongst multiple entities to allow inter-operation. e.g. a Group of controllers, e.g. each Configurator node.

Counterpart: An associated AGA12 device that, together with this device, form a pair for secure data exchange.

CM: A Cryptographic Module (defined in the US Federal Information Processing Standard FIPS 140-2) is an electronic component that is placed in-line on a communications channel and affords cryptographic protection for the communications, including, but not limited to, encryption and authentication. The class of such electronic devices is sometimes referred to as "bump-in-the-wire".

Decoding: The process of checking data is signed correctly (not tampered with) and extracting the original data from the obscured encrypted data. The algorithms for decoding are determined by the Cipher Suite and security keys. Decoding is one of the tasks carried out by the SCADAPack E RTU's Virtual SCM receiving a message from another SCM. Also see Encoding 10

Decryption: Translating Cipher Text 9 into Clear Text 9 using a cryptographic key 10. I.e. converting obscured data back into the original useful data

Default Key: Pre-assigned key or key mode (typically a factory set key 10) allowing devices to communicate "out-of-the-box". For good security, keys that are different from the default key should be used. In SCADAPack E refers to the security configuration mode for SCADAPack E Configurator keys (cf Common Key 9, Unique Key 11)

Encoding: The process of encrypting and signing data to ensure its contents are obscured and protected from tampering. The algorithms for Encoding are determined by the Cipher Suite and security keys. This is one of the tasks carried out by the SCADAPack E RTU's Virtual SCM sending a message to another SCM.

Encryption: Translating Clear Text 9 into Cipher Text 9 using a cryptographic key 10. I.e. obscuring data so that it looks random in order to hide the content of the data. Also see Decryption 10

Key: In DNP3 Secure Authentication this is also known as the Update Key and encodes dynamic session keys for authenticating devices. In AGA12 this is also known as the Encryption Key (to distinguish it from the Mac Key) 10. The Key is the common secret held by a pair of devices used for obscuring data before transmission and retrieving data from obscured data stream.

Key Pair: the combination of the Key (encryption key) and Mac Key which as a pair form the common secret held by AGA12 counterpart devices (when the Cipher Suite uses both encryption and verification signing).

Local Access Port: A dedicated, local port supporting direct connection of a DNP3 configuration terminal for local maintenance of the RTU. For RTUs using AGA12, this is the only port that communicates cleartext DNP3 and is for physically local access only. DNP3 Secure Authentication does not use the concept of a local access port on a controller (every port is secured).

Mac Key: This is the common secret held by a pair of devices and in used for digitally signing a data stream to ensure it has not been tampered with.In SCADAPack E this refers to one of the AGA12 key pairs 10.

Master Key: The master key customizes the controller security configuration file generated by the SCADAPack E Security Administrator application and is loaded into SCADAPack E RTUs that are to operate on a given customer network, or portion of a customer network.

Master Station Host: The device in a SCADA network that most remote devices report to. It typically initiates the majority of communication transactions in a network. In DNP3 Secure Authentication, the Master Station (Host) natively supports the Secure Authentication objects that are use the establish security with remote devices.

Mixed Mode: AGA12 Mixed Mode operation allows an SCM to simultaneously forward encrypted and unencrypted communications between SCADA equipment. This permits a SCADA master equipped with or connected to an SCM to communicate with a SCADA unit (e.g., RTU) that does not have an SCM. Mixed mode operation can be disabled. Mixed mode can be used for SCADAPack E AGA12 Gateway RTUs, and RTUs routing DNP3 cleartext.

Pass Phrase: In SCADAPack E the user enters this phrase to generate the Master Key 10 for a system.

Responder: A device sending authentication 9 information to a partner device in reply, to prove it is who it claims to be. See also Challenger 9.

SCM: A SCADA Cryptographic Module is a Cryptographic Module (CM) designed to or configured to operate on the communications channels between SCADA hosts and SCADA remote devices. SCADAPack E telemetry supports a Virtual SCM as part of its operating system firmware, rather than requiring an external (bump-in-the-wire) Electronic device.

SCM Configuration: Every SCM has various configuration parameters that include an SCM address, communication parameters, and static session information. SCADAPack E RTU Virtual SCMs can be configured through command line text entry, through a plug in media module (e.g. Compact Flash card on SCADAPack ES or SCADAPack ER), or through local USB peripheral communication port using SCADAPack E Configurator (SCADAPack 300E). The security files for Compact Flash card or SCADAPack E Configurator loading of the configuration is managed by a Windows® Security Administrator application.

SCM Address: SCADAPack E RTU's Virtual SCM address is obtained directly from the device's configured DNP3 node address. Every SCM on a shared or networked communications link needs to have a unique SCM address (and therefore unique DNP3 address). Addresses in the range 1 – 65519 are valid addresses for both DNP3 and SCM. Address 0 is not a valid SCADAPack E SCM address and can not be used as an SCADAPack E RTU DNP3 node address when using AGA12 security.

Security Administrator: The SCADAPack E application used by the person responsible for security administration in a network. This application is a type of security Authority 9 that retains and provides security configuration files for the rest of the system. It should be operated by corporate level security administration personnel.

Session: A session is a bidirectional virtual communications channel established between a specific pair of devices. In the case of AGA12 on SCADAPack E RTUs, a session is established between each pair of SCADAPack E virtual SCM's. A session has a type indicating it as static or dynamic. Static sessions have cryptographic and other parameters that are configured in SCM configuration data. Dynamic sessions have negotiated cryptographic parameters and vary with time and each message sent on the session. Management of sessions is one of the tasks carried out by the SCADAPack E RTU's Virtual SCM. DNP3 similarly establishes a session for communication between two devices. Part of the DNP3 session's information includes DNP3 Secure Authentication information.

SSPP: SCADA Security Protection Protocol – Defined by the AGA12-2 standard. This is the technical name of the AGA12-2 protocol that transports session information and secured data between SCMs.

Unique Key: The SCADAPack E security mode requiring that SCADAPack E Configurator nodes be individually secured (optional).

Update Key: DNP3 Secure Authentication terminology for the secret key 10 known to devices that communicate with each other.

5 Introduction

This document describes Integrated SCADA security for SCADAPack E RTU devices.

Audience

This document is for use by product users, system designers, and SCADA security administrators.

It is recommended that you have an understanding of DNP3 Secure Authentication and AGA12 Encryption.

Scope

This document contains user information as well as technical reference information. For information on configuring the Security features, refer to the *SCADAPack E Security Administrator User Manual* and *SCADAPack E Configurator User Manual*.

See the following for more information:

- ***Standards*** 13
- ***Operational Goals, Functionality Summary, & Standard RTU Operation*** 15
- ***SCADAPack E RTU Security*** 17
- ***Licensing*** 27
- ***Key Management*** 28
- ***User-based Authentication*** 33

Platforms

The following controllers support AGA12 Encryption security and DNP3 Secure Authentication:

- SCADAPack 300E Controllers
- SCADAPack ES
- SCADAPack ER

SCADAPack E Security Components

The SCADAPack E security components include the following:

- Security Administrator license file
- Security Administrator project file
- Controller Security configuration file
- SCADAPack E Configurator Security file

5.1 Standards

Standards

Security recommendations and standards of interest to utility sector markets include:

- IEC 62351
- DNP3 Secure Authentication
- AGA12 suite

The DNP3 Secure Authentication and AGA12 standards each aim to solve different security conditions. DNP3's use of IEC62351 focuses on Authentication while AGA12 focuses on Encryption.

It is widely regarded that a combination of encryption and authentication services would provide optimum protection scenarios for SCADA protocols.

IEC 62351 Standard

IEC 62351 standard specifies authentication of SCADA data transfer using digital signatures. The objectives of this standard include providing only authenticated access, stopping eavesdropping, spoofing, and playback, as well as intrusion detection. The security design specified in this standard is integrated within a SCADA protocol, requiring end-to-end implementation in order to operate.

DNP3 uses the IEC 62351 standard for Secure Authentication.

DNP3 Secure Authentication

DNP3 Secure Authentication specification is based on authentication and challenge principles. These security principles have been in place since the advent of dial-up Internet connections. These principles include Hashed Message Authentication Code (HMAC)HMAC is a calculation performed on a message. DNP3 authentication performs an HMAC on each critical message to authenticate it., in other words, prove that you are who say you are by requiring challenge-reply, a common mechanism to stop replayA replay attack is a form of network attack in which a valid data transmission is maliciously or fradulently repeated or delayed. attacks. DNP3 Secure Authentication also incorporates security "key" technology.

DNP3 Secure Authentication is designed to protect only actions that are deemed critical. This conserves bandwidth and results in only minor processing results. DNP3 Secure Authentication uses protocol Application Layer authentication when issuing the challenges, for example, controls or configuration changes. A 'signature' in the form of a security key prevents tampering but does not include data encryption. See ***How does AGA12 Work?*** 22 for information on encryption.

See the following for more information on DNP3 Secure Authentication:

- ***What is DNP3 Secure Authentication?*** 18
- ***How does DNP3 Secure Authentication Work?*** 18

AGA12 Suite

The AGA12 suite includes specific designs and reference applications for use with DNP3 as well as other SCADA protocols. AGA12 is designed to operate outside of existing SCADA protocols (specifies an additional protocol wrapper) so it s adaptable for implementation on existing systems and new

systems. External devices can be used to provide security. Typically sessions between a device external to a Master Station (e.g. gateway or other bump-in-the-wire device) and Outstations (RTUs) are secured. The IEEE is currently running projects to define AGA12 as part of substation communication security.

See the following for more information on the AGA12 suite:

- ***What is AGA12?*** 20
- ***How does AGA12 Work?*** 22
- ***Using AGA12 Security*** 33

5.2 Operational Goals, Functionality Summary, & Standard RTU Operation

Operational Goals

The operational goals of the SCADAPack E RTU's integrated security are to provide:

- Message integrity protection
- Defense against injection, modification, splicing, replay, reordering (but not Denial of-Service, although it avoids making this worse)
- Authentication
- Confidentiality
- Minimal number of messages additional to the SCADA messages, e.g., initiating sessions only when SCADA units send a message the first time, no retries and no keep-alive messages

Functionality Summary

The Integrated Security functionality provided by the SCADAPack E RTUs includes Secure Authentication with optional, integrated user credentials and maintenance software security.

Protection is provided on DNP3 communication ports operating on short-range (local) and long-range (remote) links.

DNP3 Secure Authentication is provided to v2 of the DNP User Group Secure Authentication standard. AGA12 Encryption for DNP3 is provided to the AGA12-2 recommendations.

DNP3 Secure Authentication and AGA12 Encryption security on SCADAPack E RTUs applies only to DNP3 communications. The following SCADAPack E RTU communications media support security:

- DNP3 RS232 serial ports
- Hayes Modem dial-up connections (DNP Secure Authentication only)
- DNP3 RS422 serial ports
- DNP3 RS485 serial ports
- DNP3 / IP communications (TCP and UDP), including Ethernet, PPP, GPRS, 1xRTT, etc.
- USB local connection (SCADAPack 300E controllers only)

Security is a licensed feature of SCADAPack E RTUs. When the controller is licensed for Encryption AGA12 or Authentication SAv2, security operation is activated when a security configuration file is loaded in to the device. The security configuration file is generated by the SCADAPack E Security Administrator application.

Standard RTU Operation

Secure communications is enabled on a device when a security configuration has been loaded on the RTU for the first time.

If a security configuration has not been loaded in to an SCADAPack E RTU, security will not be active on its DNP3 ports, and the RTU operates in its standard (non-secured) way.

I.e. communications will operate as standard DNP3 on DNP communication ports until a security configuration is loaded for the the first time. When operating this way, the RTU ports are referred to as

Standard DNP3 Ports.

5.3 SCADAPack E RTU Security

- *What is DNP3 Secure Authentication?* 18
- *What is DNP3 Secure Authentication?* 18
- *How does DNP3 Secure Authentication Work?* 18
- *What is AGA12?* 20
- *How does AGA12 Work?* 22
- *Supported AGA12-2 Functionality* 22
- *How do AGA12 encyption and DNP3 Secure Authentication Work?* 24
- *Highlights of* 24 *SCADAPack E RTU Security* 24

5.3.1 What is DNP3 Secure Authentication?

DNP3 Secure Authentication is a bi-directional protocol that adds data integrity protection and user and device authentication, resulting in protection between master stations (HMI, control servers), outstations (PLCs, RTUs, IEDs) and Configuration software using the DNP3 protocol.

SCADAPack E RTUs support DNP3 Secure Authentication to the DNP User Group Secure Authentication Specification v2.00

For more information, see:

- ***How does DNP3 Secure Authentication Work?*** 18

5.3.2 How does DNP3 Secure Authentication Work?

DNP3 protocol specifies data link, transport, and application layers. DNP3 Secure Authentication operates at the application layer. This means that DNP3 transactions are secured from end to end through a system regardless of the communications protocol specified (TCP/IP, UDP/IP, serial) and independent of the presence of communications gateways, routers, etc. It also means DNP3 can be secured in hybrid networks, for example, through TCP/IP then to serial communications.

DNP3 Secure Authentication takes place in three scenarios:

- ***Initialization*** 18
- ***Periodic*** 18
- ***Critical Function Code Requests*** 18

Initialization

When initiating a session, DNP3 Secure Authentication authenticates that the master station and outstation are who they claim to be. This scenario is designed to prevent spoofing, replay, and other forms of cyber attacks. This is accomplished using a unique session key (dynamic) derived from the pre-shared secret keys known by both devices (static Update key).

Periodic

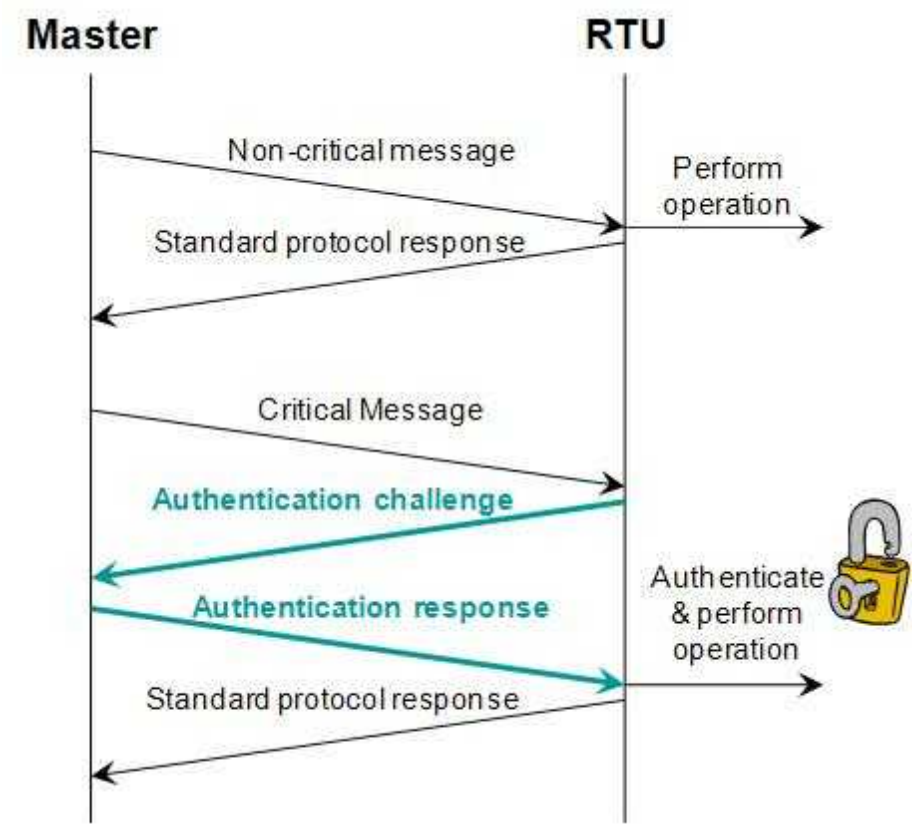
Once a session is established, the master station and outstation periodically verify again who they claim to be to prevent hijacking and other attacks. The default SCADAPack E authentication period is 30 minutes. The maximum periodic authentication period is 14 days. A new (dynamic) session key is generated and exchanged during each periodic update.

Critical Function Code Requests

Messages that are regarded as "critical" operations are challenged by the receiver, asking the requester for security credentials. The receiver needs to gain confidence that the requester is who he says he is, before proceeding to perform the request.

Both non-critical and critical message transactions are shown in the picture to illustrate the difference between the unchallenged message, whose operation is the same as the standard DNP3 protocol without security, and the challenged message that utilizing the DNP3 Secure Authentication mechanism.

See Challenged Functions 36 for a list of the critical function codes challenged by the SCADAPack E RTU.

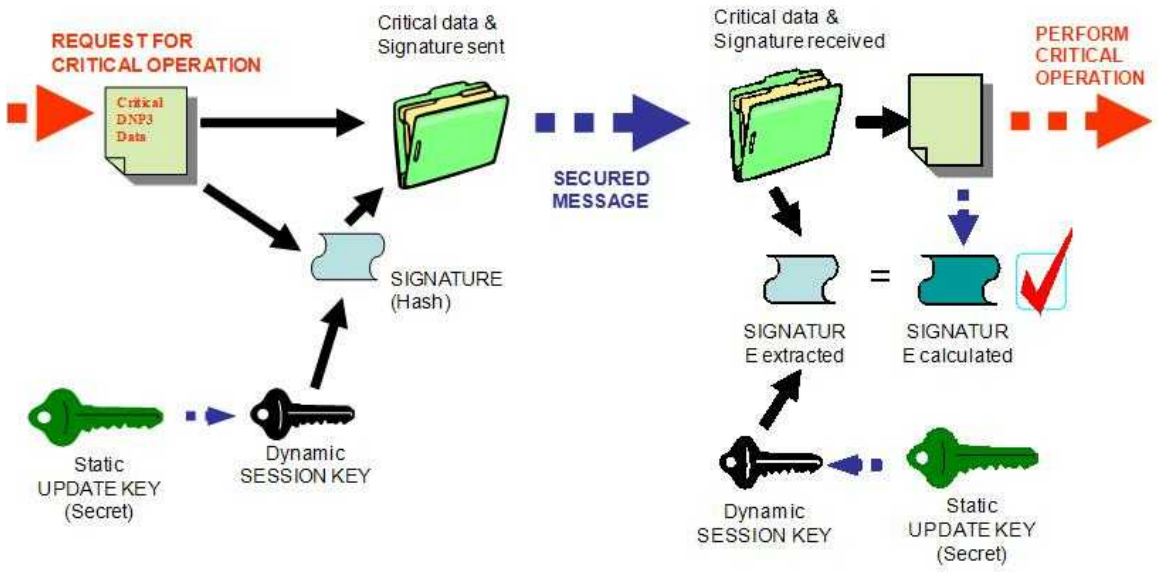


Further transaction scenarios are detailed in the DNP3Specification Volume 2 Supplement 1 - Secure Authentication document available to DNP User Group members. See www.dnp.org

Use of Security Keys

DNP3 Secure authentication uses a cryptographic key technically known as the "Update Key" for securing messages. This static key is the pre-shared "secret" between a master device and the outstation device.

From the Update key, a dynamic "Session Key" is created that protects critical operational data. A summary of this data flow is shown in the following picture.



This data flow applies to DNP3 security initialization 18, periodic 18 key changes and challenged critical requests 18.

Aggressive Mode

The data flow described in the above picture also applies to DNP3 Aggressive Mode 41 transactions.

Once security credentials are established through a previous critical request 18, aggressive mode allows the challenge data to be appended to the critical request message without having to go through the full challenge / reply exchange, as shown in the following picture.

5.3.3 What is AGA12?

The American Gas Association (AGA), in a project for the Gas Technology Institute, formed a working group to develop a cryptography standard to protect SCADA data communications from cyber attacks. The working group developed AGA12, which is a suite of cryptography standards that recommend how to achieve this.

The AGA12 standard consists of four documents. Each document addresses different aspects of SCADA data transmission protection. AGA12-2 details the requirements to build interoperable cryptographic modules to protect SCADA communications for low-speed legacy SCADA systems and maintenance ports. AGA12-2 is one component of cryptographic protection for SCADA communications.

AGA12-2 specifically defines a protocol (SSPP) for use in establishing connection, transporting, encrypting and signing serial SCADA protocols including DNP3. It also defines its operation on a device known as a SCADA Cryptographic Module (SCM).

AGA12 includes specific designs and reference applications for use with DNP3 as well as other SCADA protocols. AGA12 is designed to operate outside of existing SCADA protocols because AGA12 specifies and additional protocol wrapper. It is adaptable to implement on existing systems and new systems.External devices can be used to provide security. Typically sessions between a device external

to a master station, for example, gateway or other bump-in-the-wire device (BITW) and outstations (RTUs) are secured.

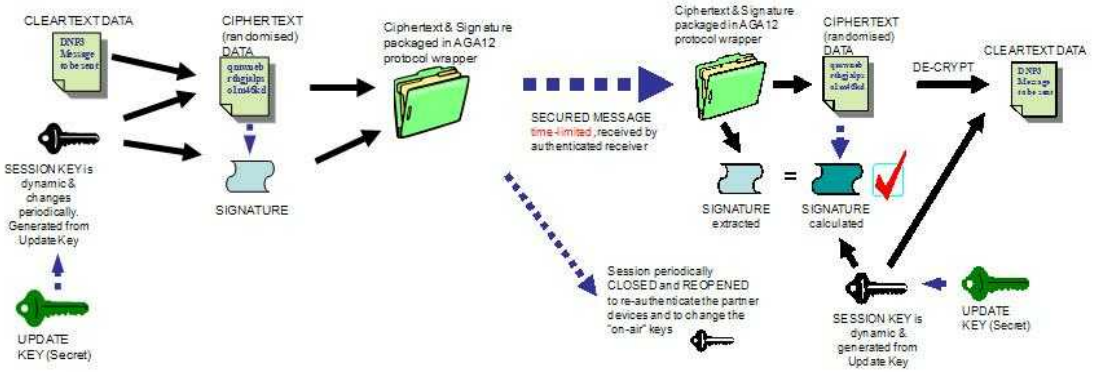
SCADAPack E RTUs support AGA12-2 protocol through a Virtual SCADA Cryptographic Module (SCM), integrated with the various operational aspects of the RTU. The implementation adheres to the AGA12-2 recommendations and inter-operates with the AGA12-2 reference application. It is for interoperabilitye with other AGA12-2 compliant devices.

See the following sections for more details:

- ***How does AGA12 Work?*** 22
- ***Using AGA12 Security*** 33

5.3.4 How does AGA12 Work?

The AGA12 suite uses cryptography to protect SCADA communications. Essentially, it provides a means to take clear text messages and convert them into unintelligible forms (ciphertexts) using a secret number. These encrypted messages can be sent over an insecure connection without the threat of interception and being read by a user or device other than that to which the message was sent. Once the message arrives at its secure location, it is deciphered using the same secret number. This secret number is called a key. The figure below illustrates how an AGA12 message is handled during the encryption and decryption processes:


CLEAR TEXT DATA
CIPHER TEXT (randomised) DATA
Ciphertext & Signature packaged in AGA12 protocol wrapper
SESSION KEY is dynamic & changes periodically. Generated from Update Key
SIGNATURE
UPDATE KEY (Secret)
SECURED MESSAGE time-limited, received by authenticated receiver
Ciphertext & Signature packaged in AGA12 protocol wrapper
CIPHER TEXT (randomised) DATA
DE-CRYPT
CLEAR TEXT DATA
SIGNATURE extracted
=
SIGNATURE calculated
Session periodically CLOSED and REOPENED to re-authenticate the partner devices and to change the "on-air" keys
SESSION KEY is dynamic & generated from Update Key
UPDATE KEY (Secret)

AGA12 incorporates security key technology. This technology is based on open cryptography standards, for example, AES encryption. As well as encrypting data content with security keys, AGA12 validates connections between users using secret keys. The use of these keys allows AGA12 to protect messages by authenticating partner devices and randomizing transactions between the devices.

AGA12 defines a device as a SCADA Cryptographic Module (SCM).

For more details on how AGA12 works, see:

- ***Description of Security Facilities*** 35
- ***Using AGA12 Security*** 33

5.3.5 Supported AGA12-2 Functionality

Notable AGA12-2 standard functionality provided in the SCADAPack E RTU includes:

- SSPP (SCADA Security Protection Protocol): The 'SCM address' is equated with the existing 'DNP3 node address' to reduce configuration effort. The SCADAPack E RTU routing architecture already requires uniqueness. DNP3 provides node addresses in the range 0-65520. SSPP allows SCM addressing in the range 1-65535. The unique address range that should be used for DNP3 / SCM addressing is: **1-65520**. A limited ability to override a destination SCM address is provided, primarily to permit AGA12 Gateway operation (i.e. the destination of RTU messages is typically the Master Station DNP3 address and is different from the SCM address of the AGA12 Gateway).
- Ciphersuites (encryption algorithm / hash algorithms) supported are:
- AES128-CTR / HMACSHA-1 (suite 1)
- AES128-CTR / HMACSHA-256 (suite 4)
- Suite 1 uses 128-bit encryption with 160-bit verification signing, while suite 4 uses 128-bit encryption with 256-bit verification signing. Suite 4 provides better security but more computation.

- Concurrent mixed mode operation of cleartext DNP3 protocol and AGA12-2 SSPP protocol on the same link, for DNP3 (& SSPP) routing and AGA12 Gateway operation.
- Static session negotiation for dynamic session exchanges (standard AGA12)
- Dynamically changing on-air keys for maximum protection
- Association numbers, Session ids, validity time windows (standard AGA12)
- Fixed signaling character and byte-stuffing characters (as per AGA12-2 reference application for DNP3)
- Counterpart List detailing nodes permitted to interact with this node, key definitions, time windows
- Communication synchronization to re-establish AGA12 sessions following expiry of sessions (standard AGA12 feature)

Omissions

The SCADAPack E RTU does not currently provide the following AGA12-2 facilities:

Selection of AES128-CBC mode (Cipher Block Chaining) and session establishment BEG message [AGA12-2 changes from March 2006]. These will be supported in a future version of the SCADAPack E RTU.

Selection of AES128-PE (low SCM latency, high computation variant of AES encryption). This methodology is useful for SCM “bump in the wire” external devices to minimize re-transmission latency. This is not a consideration where systems deal with only remote SCADAPack E RTU’s Virtual SCM devices, as there is no serial retransmission of cleartext messages. Where the SCADAPack E RTU AGA12 Gateway transmits cleartext data, this is typically at a higher data (e.g. via Ethernet). AES128-PE may be supported in a future version of the SCADAPack E RTU.

Selectable signaling characters and byte-stuffing characters. These are not available for user configuration, rather fixed as per the description in Section ***Fixed AGA12-2 Parameters*** 63.

BROADCAST or MANAGEMENT dynamic or static session data. Management session handling may be provided in a future version of SCADAPack E RTU.

SCM Bank support (for modem banks)

Instruct an SCM to establish a dynamic session – manually forcing a session to open to another SCM device is not supported

RCA, CAR commands (address request & response) are not supported by the SCADAPack E RTU

Optimization of SSPP operation for PSTN and other long-connection-establishment media. This may be provided in a future version of SCADAPack E RTU.

5.3.6 How do DNP3 Secure Authentication and AGA12 Encryption Work together?

When used together, AGA12 provides the encryption and session validation security facilities, while DNP3 Secure Authentication provides the challenge-reply authentication security facilities. Both AGA12 and DNP3 Secure Authentication standards are relevant to DNP3 communications and SCADAPack E RTUs.

To suit retrofit of existing systems, AGA12 and DNP3 Secure Authentication can be configured without affecting the control system infrastructure and without an interruption in the system's operation. Retrofits can be achieved without compromising communications between the RTUs and master stations.

5.3.7 Highlights of SCADAPack E RTU Security

- For security management, a Security Administrator application allows the creation of a security management collection, containing security configuration for a whole system. It can generate Master Key file, RTU security configuration files, and SCADAPack E Configurator security files. These can be written directly to a media interface.
- Generally system security is setup in the following ways:

  1) have unique security keys for each remote RTU that communicates only with the master station host (most secure), or

  2) have a common security key across a *Group* of controllers that interact together or are in some collection with the master station host (e.g. Northern RTU sites). Different groups have unique security keys (pretty good security)

  3) have a common security key across a whole system, i.e. one *Group* (most convenient, but least secure)

  Option 1 has the benefit that someone learning one key does not have access to the whole system. Similarly, Peer nodes can be restricted as to what other Peer nodes they can talk to. This provides maximum security but means additional management of keys.

  Option 3 is simpler to manage, but if the common key becomes known, all RTUs are compromised.

  Option 2 is a compromise offering pretty good securty, but may be necessary where there is interaction between peer RTUs (for example). SCADAPack E DNP3 Secure Authentication or AGA12 Encryption requires that all interacting devices share the same keys (e.g. RTU 1 & 2 communicate Peer-to-peer, both talk to a master station host. All 3 devices need to use the same key in this case).

- Licensed RTUs can operate as end-nodes receiving AGA12 encrypted DNP3 frames and responding with AGA12 encrypted DNP3 frames. Similarly they can operate send and receive DNP3 Secure Authentication messages.
- RTUs can be DNP3 and AGA12 routers on any communications media. No special configurations are required for this. A router passes on AGA12 frames or DNP3 secure authentication frames. This is particularly useful for wide area radio networks.
- SCADAPack E RTUs also support encryption of Unsolicited, Peer DNP3 and DNP3 Master (data concentrator) transmissions with both DNP3 Secure Authentication and AGA12 encryption security.

- Remote configuration of security parameters can be granted through the Security Administrator to allow security configuration files to be loaded remotely. This feature can be disabled for increased security protection. In this case it is only possible to configured security through the following mechanisms:

  - Compact Flash card plugged in to SCADAPack ES or SCADAPack ER RTUs (with security configuration files loaded)

  - via SCADAPack E Configurator to SCADAPack 300E via USB peripheral communications

- Configuration files containing the security keys and other security parameters can be put on a media interface for direct deployment to RTUs (e.g. Compact Flash card for SCADAPack ES / SCADAPack ER), USB memory stick for loading to a controller by SCADAPack E Configurator, etc). Depending on the arrangement of RTU groups, this allows multiple RTUs to be configured from the same single media ("Security Key"). In the case of SCADAPack ES / SCADAPack ER, a Compact Flash card could be plugged in & removed from each RTU in the same *Group* in turn.

- DNP3 Secure Authentication diagnostics and AGA12 Diagnostics are available through the SCADAPack E RTU diagnostic mechanisms (serial diagnostic port, Telnet, diagnostic file capture).

DNP3 Secure Authentication

- A mixture of unsecured DNP3 devices and DNP3 Secure Authentication devices can coexist on the same network. The Master station needs to be aware of the configuration requirements of individual devices, which includes security configuration.
- SCADAPack E Configurator can communicate directly to devices configured with DNP3 Secure Authentication, providing the SCADAPack E Configurator node and user is authorized (configured by the Security Administrator and loaded to devices).
- Where both AGA12 and DNP3 Secure Authentication is configured, communication from SCADAPack E Configurator nodes connected remotely on the network can optionally require SCADAPack E Configurator nodes and users to be authorized, but requires communications to be routed via an AGA12 Gateway RTU.
- SCADAPack E Configurator Security can be setup in a number of ways:

  A) optionally require the use of individual Username / Password logins to authenticate with RTUs. Username/password lists are configured in all RTU devices in this case.

  B) Choose one of three SCADAPack E Configurator Security modes:

  B.1) Default Key mode - where the Configurator and RTUs will communicate out-of-the-box (most convenient but least secure)

  B.2) Common Key mode - where a new key is provided to all Configurators and all RTUs, disabling the user of the Default Key and configuring a single specific key (convenient with better security)

  B.3) Unique Key mode - where all Configurators have an individually unique key and all RTUs are aware of the authorized configurators (best security)

AGA12 Encryption

- SCADAPack E RTUs support defining a SCADA Cryptographic Module (SCM). This AGA12 functionality is integrated with the RTU's serial port communication drivers, DNP3 stack, and IP stack.
- To provide AGA12 encryption features or DNP3 Secured Authentication, a controller feature licence 27 needs to be installed.
- RTUs can be setup to operate in AGA12 *GATEWAY* mode, receiving cleartext DNP3 and encrypting to AGA12 prior to transmission on a communications channel. Conversely a gateway can receive

encrypted DNP3 response frames and decipher them to cleartext DNP3 for transmission back to the requester. Typically this gateway mode is used via serial or network links for host system communications. Gateway mode can be used for central maintenance access to remote RTUs and for DNP3 masters not supporting integrated AGA12 functionality.

- Communication networks can operate in AGA12 *MIXED MODE* as described by the AGA12-2 standard, allowing a mixture of cleartext DNP3 and encrypted AGA12 frames to operate on the same network. Gateways setup to operate in *MIXED MODE* allow the user to decide if the risk profile for some RTU's indicates they aren't worth securing and therefore can continue to run in cleartext DNP3. This also allows systems to be transitioned from cleartext DNP3 to secure AGA12 systems in a planned migration strategy.
- Encrypted data is supported on multiple communications media: direct serial / keyed serial / Ethernet (UDP / TCP) / GPRS / 1xRTT. AGA12 Encryption for PSTN is not currently supported in SCADAPack E RTUs. DNP3 Secure Authentication can operate with PSTN communications.
- Every RTU configured with AGA12 security provides a Local Access port. The provides communication using cleartext DNP3 - this is primarily for use of SCADAPack E Configurator, but may also be used by other devices locally [securing this port is a physical security issue]. All other RTU DNP3 ports are AGA12 encryption protected (for routing, backup links, etc) when AGA12 security is configured.
- SCADAPack E Configurator and other package(s) using DNP3 protocol can communicate with remote protected RTUs through a central AGA12 Gateway RTU.

5.4 Licensing

To license either DNP3 Secure Authentication or AGA12 Encryption for DNP3, you need a controller feature licence. Typically, this is done when the controller is purchased, although a controller feature licence can be purchased and added at a later time. The controller feature licence file is deployed using SCADAPack E Configurator.

For more information on licensing RTUs, see the *SCADAPack E Telemetry Operational Reference* manual.

5.5 Key Management

- *SCADAPack E Configurator Key Mode* 29
- *Configurator Key Mode* 29
- *Compact Flash Entry and UTIL LED* 31
- *Local USB Configuration* 32

5.5.1 SCADAPack E Configurator Key Modes

There are three modes for security keys when securing access from SCADAPack E Configurator to SCADAPack E controllers. These modes are:

Default Key Mode

The default key mode is the easiest option to use and maintain. The disadvantage of using a default key is the same as its convenience: it works out-of-the-box, and so it provides the weakest level of security.

The advantage of this mode is that there is no need to manage Configurator security files because the secret key is known by SCADAPack E controllers and SCADAPack E Configurator, by default. It does help with protecting against external attempts to access the protocol, but not against copies of the SCADAPack E Configurator software. This mode does, however, still allow user-based authentication to be selected in SCADAPack E Configurator and the controller as a separate layer of security.

The default key mode is provided for simplifying initial access to controllers, however it is strongly recommended that you not use the factory default key mode in field installations.

Common Key Mode

To simplify key management for small systems, the common key mode provides more security than the default key mode. The common key mode requires that the same Configurator security configuration file be deployed to every instance of SCADAPack E Configurator. The advantage of this is that it means you only have to maintain one key for all of your SCADAPack E Configurator installations. The disadvantage of this is that if a laptop with SCADAPack E Configurator is compromised, the security configuration files needs to be updated on all instances of SCADAPack E Configurator, as well as on every controller that is associated with SCADAPack E security features.

The common key is generated as part of the Security Administrator project settings. Like the default key and unique key modes, this option does allow user-based authentication in SCADAPack E Configurator and the controller.

Unique Key Mode

The unique key mode provides the highest level of security. Each instance of SCADAPack E Configurator is identified using a specific security configuration file. This file is tied to a Machine ID to restrict operation of the software to authorized PCs only. You can add, edit, or remove instances of SCADAPack E Configurators from the system, but similarly needs to update every controller with revised settings. The Security Administrator generates a unique security key for each instance of SCADAPack E Configurator.

An advantage of using this mode over the common key mode is that if a laptop is compromised, there is no need to update the security configuration file for each instance of SCADAPack E Configurator. You can remove the compromised SCADAPack E Configurator from the Security Administrator and new controller security configuration files can be generated and deployed to the RTUs.

5.5.2 Master Key Configuration

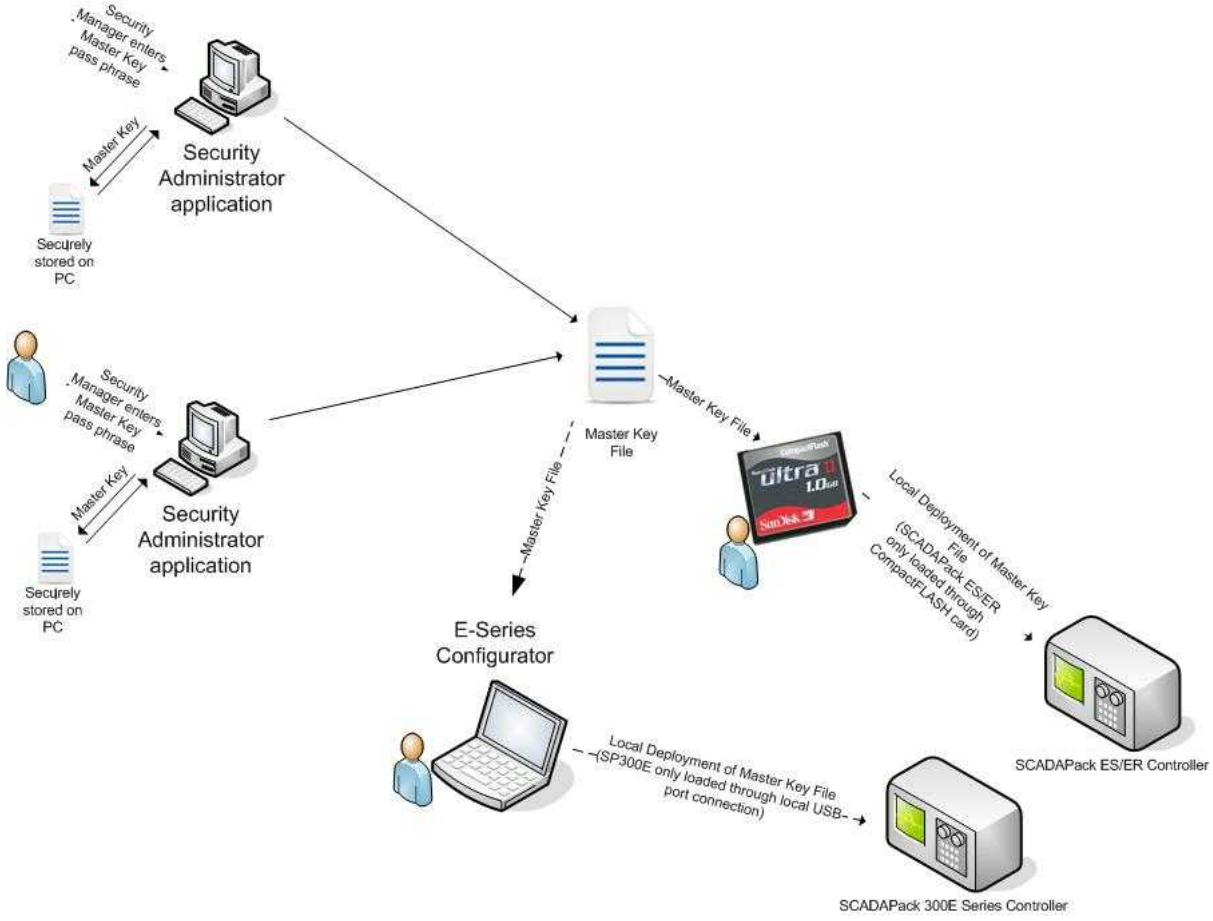
The security infrastructure is designed so that master keys are deployed once during the lifetime of a system from the Security Administrator application to controller devices.

It is highly recommended that a trusted individual responsible for system security deploy the master keys to controller devices before releasing them for field installation.

Copies of the master key file need to be removed from portable media and devices following deployment. To ensure the integrity of the security system, you need to take all possible steps to keep the password phrase, master key file, and its deployment secure.

To deploy a generated master key file to SCADAPack ES or SCADAPack ER controllers, you need to do so from a CompactFLASH card. You cannot deploy it from the Security Administration application.

To deploy a generated master key file to a SCADAPack 300E controller, you need to use SCADAPack E Configurator through the USB peripheral port.


Security Manager enters Master Key pass phrase
Master Key
Security Administrator application
Securely stored on PC
Security Manager enters Master Key pass phrase
Master Key
Security Administrator application
Securely stored on PC
Master Key File
Master Key File
Master Key File
Local Deployment of Master Key File (SCADAPack ES/ER only loaded through CompactFLASH card)
E-Series Configurator
Local Deployment of Master Key File (SP300E only loaded through local USB port connection)
SCADAPack ES/ER Controller
SCADAPack 300E Series Controller

The master key contains the security boundary for RTUs and security administration for one organization or a part of an organization. What the master key does is that it customizes the controller security configuration file that the Security Administrator generates so that the file is system or organization specific. The RTU reads this information.

If required, the Security Administrator can generate new master keys. This is done by entering a new pass phraseUsing a one-way has function to transform an arbitrary length test string ito a psuedo-random bit string is a technique called key crunching. The text string is often referred to as a pass phrase (sometimes written as passphrase). The reason for using passphrases is the avoidance of ever recording un-encrypted keying information, to prevent its compromise. . It is a critical piece in the security chain and needs to be kept secret. Whenever you enter the pass phrase, you need to enter it exactly the same each time.

The pass phrase is stored on the security administration computer independently of the Security Administrator project. The pass phrase needs to be re-entered on every Security Administrator you have installed.

In addition, the Security Administrator provides the means to export a master key file. The master key file is called system.key.

When you choose to generate a new master key, you will need to update the master key locally at each RTU device using this key (as described above and shown in the picture).

5.5.3 Compact Flash Entry and UTIL LED

Using Compact Flash to load security configuration is supported by the following RTU hardware:

- SCADAPack ES
- SCADAPack ER

Security Configuration for these devices can be loaded from a file on the plug-in media “security key” (i.e. CompactFlash card). Insertion of a card in to the SCADAPack E RTU is automatically detected.

If security is licensed on the RTU, the media root directory is checked for the security configuration file:

SYSTEM.RTK

If the RTU does not find this file, the RTU encryption information remains unchanged.

Like KEYS for a door or any other form of security, safe-keeping and distribution of AGA12 keys is necessary.

UTIL LED

The SCADAPack ES and SCADAPack ER RTU hardware includes a "UTIL" LED that indicates the state of a completed operation on the Compact FLASH Utility port.

Upon successfully loading a security configuration file from the Compact FLASH port the "UTIL" LED flashes alternately on and off at a steady rate for 5 seconds.

5.5.4 Local USB Configuration

The following RTU hardware allows the use of USB peripheral interfaces, locally, for security configuration entry:

- SCADAPack 300E RTUs

Security Configuration for these devices can be loaded using the USB peripheral interface and SCADAPack E Configurator, from a security configuration file generated by the Security Administrator.

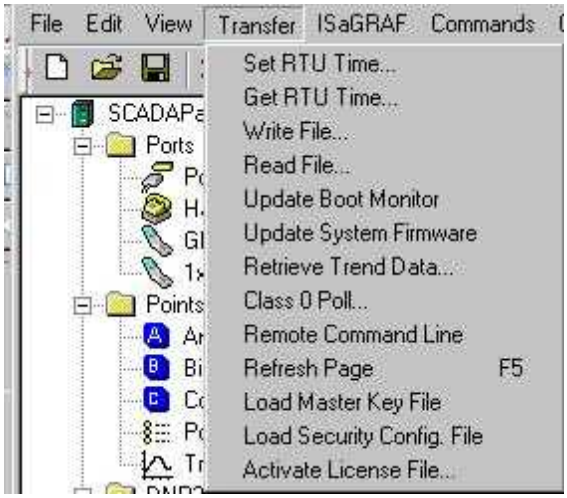
This file is called:

SYSTEM.RTK

Like KEYS for a door or any other form of security, safe-keeping and distribution of security keys is necessary.

SCADAPack E Configurator

For SCADAPack 300E RTUs, SCADAPack E Configurator provides a facility for loading the security configuration file through the USB interface. Use the *Transfer > Load Security Config. File* menu item to do so. It prompts you to choose the security configuration file.



5.6 User-based Authentication

This feature is only available when DNP3 Secure Authentication is licensed and configured.

To enhance security when multiple SCADAPack E Configurator users are present in a system, the Controller Security configuration file can include a user list.

The SCADAPack E Security Administrator application allows configuration of users, providing a list of the usernames (and passwords associated with the usernames). This is configured in RTUs using the Group security configuration files.

The User-based authentication feature uses the SCADAPack E RTU to act as an authentication server for access requests from SCADAPack E Configurator. When an access request is received from the SCADAPack E Configurator, the RTU uses DNP3 Secure Authentication keys and the usernames and passwords.

When a user accesses a system using SCADAPack E Configurator with User-based Authentication enabled, username and password credentials are entered into SCADAPack E Configurator. The controller verifies that the username and password match the information entered on the security configuration user list. When this information matches, the user is authenticated and the action is permitted. If the information does not match, the controller rejects the attempted action and SCADAPack E Configurator displays a message.

6 Telnet and FTP Authentication

The Telnet and FTP applications provided on SCADAPack E as part of the IP management suite can be insecure if not externally secured. This is because transmissions in these TCP/IP application protocols transmit their data, including usernames and passwords, in clear text 9.

It is strongly recommended that Telnet and FTP are DISABLED when not in use. Leaving these two applications enabled creates a security vulnerability if the remote IP connection to an RTU is not secured using another means.

To determine if your Telnet and FTP settings are enabled, check the SCADAPack E Configurator *TCP/IP* property page.

7 Using SCADAPack E Security

The following sections describe configuration and the use of SCADAPack E security facilities.

An individual RTU's security settings can be configured by plugging a media interface into the RTU, for example, a CompactFlash card (for SCADAPack ES and SCADAPack ER) or by direct location connection of SCADAPack E Configurator through a USB peripheral port, for example, for SCADAPack 300E RTUs).

Alternatively, the Security Configuration may permit it to be loaded remotely. This allows remote maintenance of security configurations from SCADAPack E Configurator and Master Station Host systems such as ClearSCADA.

See Section ***Security Administration*** 69 for information on Security Administration and plug-in media.

- ***Description of Security Facilities*** 35
- ***DNP3 Secure Authentication*** 36

- ***AGA12 Encryption*** 44
- ***Security Considerations*** 68

7.1 Description of Security Facilities

In general terms, security facilities are provided using the following mechanisms:

- a system using DNP3 Authentication is secured through Groups where a security key (Group's Common Key) is shared between outstations and the Master Station Host (requires DNP3 Secure Authentication at the master station);
- a system using AGA12 is secured using SCM (SCADA Cryptographic Module) devices. In the case of SCADAPack E RTUs, a virtual SCM 10 is integrated with the RTU (this operates via an AGA12 Gateway RTU independent of the master station);
- a system using DNP3 Authentication and AGA12 Encryption concurrently is secured using an AGA12 Gateway RTU and Master Station Host supporting DNP3 Secure Authentication. The common Group key and AGA12 Encryption Key is used by the outstation and the AGA12 Gateway RTU. The Group key is used by the Master Station Host and RTUs.

The Security Administrator application is used to generate Security Configuration files for SCADAPack E controllers and SCADAPack E Configurator nodes.

7.2 DNP3 Secure Authentication

DNP3 Secure Authentication operates at the DNP3 Application Layer.

Where Master Station Host to RTU controller security is desired, the Master Station Host must natively support DNP3 Secure Authentication.

Licensing and enabling DNP3 Secure Authentication on the SCADAPack E RTU secures DNP3 interfaces (serial ports, Ethernet ports, USB on SCADAPack 300E RTUs), including communication with SCADAPack E Configurator software.

SCADAPack E RTUs support DNP3 Secure Authentication when operating as a Data Concentrator communicating with remote outstations.

SCADAPack E RTUs also support DNP3 Secure Authentication when operating with peer to peer communications with other outstations.

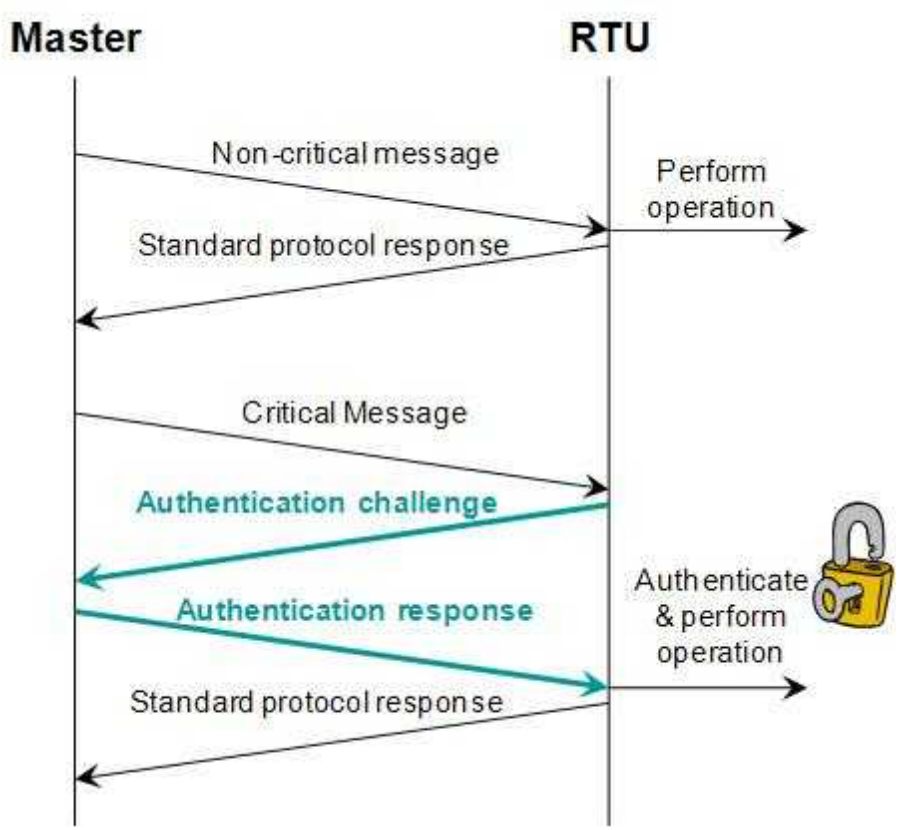
SCADAPack E Data Concentrator and Peer communication security relies on inter-communicating devices to be in the same security Group. i.e. use the same security keys to configure their communication. For example, the same key value needs to be used at the Master Station host, data concentrator, remote RTUs, as part of the same Group.

DNP3 Secure Authentication operates using a Challenge / Response security model. Critical operations are challenged by a node when it receives a message to perform a critical operation.

- ***Challenged Functions*** 36
- ***DNP3 Security Settings*** 38
- ***Aggressive Mode*** 41
- ***Vulnerabilities Addressed*** 43

7.2.1 Challenged Functions

When DNP3 Secure Authentication is active on an SCADAPack E RTU, it challenges the mandatory DNP3 (critical) function codes and several of the DNP3 optional function codes. I.e. The RTU challenges the operation of a rejecter whenever it sends any of these function codes. (Requester could be a Master Station host, Data Concentrator, Peer device or Configurator tool).



The following DNP3 function codes are challenged by the SCADAPack E RTU when received from a Master device:

DNP3 Function Code	
2	Write
3	Select
4	Operate
5	Direct Operate
13	Cold Restart
14	Warm Restart
15	Initialize Data
20	Enabled Unsolicited Responses
21	Disable Unsolicited Responses
22	Assign Class
24	Record Current Time

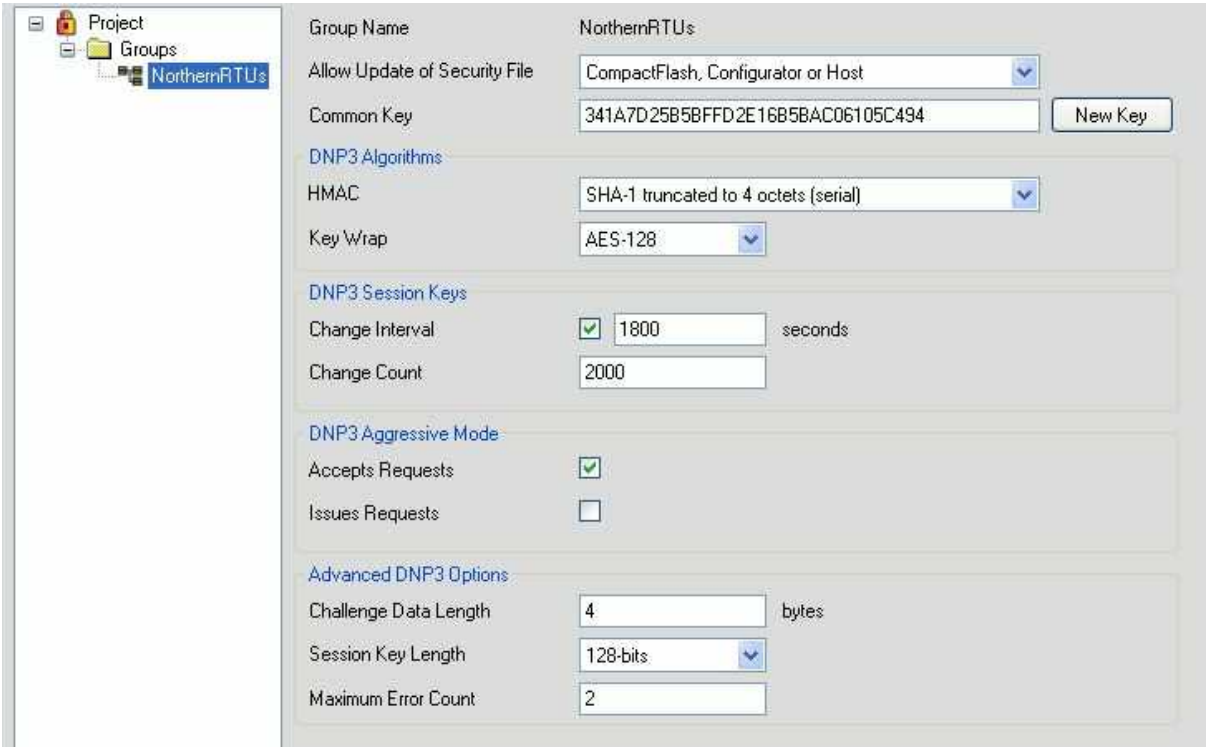
25 Open File

27 Delete File

7.2.2 Security Settings

A number of security settings can be adjusted by the Security Administrator for DNP3 Secure Authentication interoperability and security performance.

Security settings for the SCADAPack E controllers are set on the Security Adminstrator's **Group** page.



Allow Update of Security File

Common Key

This is the security key (static DNP3 Update Key) common to devices in this security Group. It can be generated by the Security Administrator application or generated externally and entered in this field on the Security Administrator.

Devices that use this key may include Master Station Host, Data Concentrators, Remote RTUs and IEDs, Peer RTU devices.

(This key is also used by AGA12 Encryption 44)

DNP3 Algorithms

HMAC

This is the security algorithm used for "signing" security messages to confirm they have not been tampered with. The setting of this field needs to be the same on each device using the Common Key 38. This setting applies to DNP3 interfaces on the SCADAPack E RTU.

Choose one of the algorithms:

- SHA-1 truncated to 4 octets (serial)
- SHA-1 truncated to 10 octets (networked)
- SHA-256 truncated to 8 octets (serial)
- SHA-256 truncated to 16 octets (networked)

The SHA-256 algorithms are more secure than the SHA-1 algorithms but are more RTU processing intensive. Algorithms with more octets are more secure, but cause longer messages (using more bandwidth) for critical messages.

It is recommended to use one of the algorithms with a *(serial)* indicator where the primary communications interface protection is being deployed on is DNP3 serial ports.

It is recommended to use one of the algorithms with a *(network)* indicator where the primary communications is a network interface (Ethernet, PPP, etc).

Key Wrap

This is the security algorithm used for encrypting the security exchanges that set the dynamic session key from the static DNP3 Update Key. The setting of this field needs to be the same on all devices using the Common Key 38.

Only the AES-128 algorithm is presently supported.

DNP3 Session Keys

These settings control how the session key regularly changes (also known as key rotation). Changing the session key is a very large part of security strategy. It stops large volumes of data using the same cryptographic parameters (which can lead to the ability to learn the session key).

Session keys will be renegotiated when either of the Change Interval or Change Count criteria is met. Whichever criteria is met first will cause the renegotiation, then checking for both criteria is restarted.

Change Interval

When enabled, this interval sets the time period for which the DNP3 dynamic session key is valid. After this time, the session key is renegotiated.

Change Count

This is the number of times a session key can be used before it is renegotiated.

DNP3 Aggressive Mode

Accepts Requests

Determines whether the controller will accept Aggressive Mode requests from a master device sending critical controls. If Aggressive Mode is disabled, then an aggressive mode request will the rejected by the RTU. The master should use, or be configured to use, standard challenge-reply security messages in this case. The setting of this field needs to be the same on each device using the Common Key 38.

See Aggressive Mode 41 for more information.

Issues Requests

Determines whether the controller will send Aggressive Mode requests when communicating as a DNP3 Master (e.g. Data Concentrator to remote outstations or IEDs, Peer-to-peer with another RTU). This setting applies to communications initiated by the RTU. If a remote device rejects an aggressive mode request, authentication will be unsuccessful. Disable the Aggressive Mode - Issues Requests setting if there are authentication issues. The setting of this field must be the same on all devices using the Common Key 38.

See Aggressive Mode 41 for more information.

Advanced DNP3 Options

Challenge Data Length

This sets the number of bytes of pseudo-random challenge data used in session key negotiation and authentication challenge messages.

The minimum length of challenge data is 4 octets. The maximum SCADAPack E length for challenge data is 40 octets. The larger the challenge data the better the security but the more overhead on security establishment and challenge messages.

The setting of this field needs to be the same on each device using the Common Key 38. This setting may be a global setting on some devices, thereby requiring a whole system to operate with the same value.

Session Key Length

The size of the dynamic session key used in session key negotiation and protecting critical message challenges.

The minimum length of session keys is 128-bits (16 octets).

The session key length can be selected from one of the following on the SCADAPack E RTU: 128-bits, 192-bits, 256-bits, 384-bits, 512-bits, 1024-bits.

The larger the session key the better security, but large session keys have more overhead on security establishment, and are more RTU processing intensive.

The setting of this field needs to be the same on each device using the Common Key 38.

Maximum Error Count

This sets the number of consecutive security conditions for which the SCADAPack E RTU will return errors. After this number of errors, security conditions are silently discarded. This mechanism attempts to alleviate denial of service issues.

In a noisy network environment it may be necessary to increase this count for consistent security exchanges. The higher this number the more prone the communications is to disruption if a device is subject to denial of service incident.

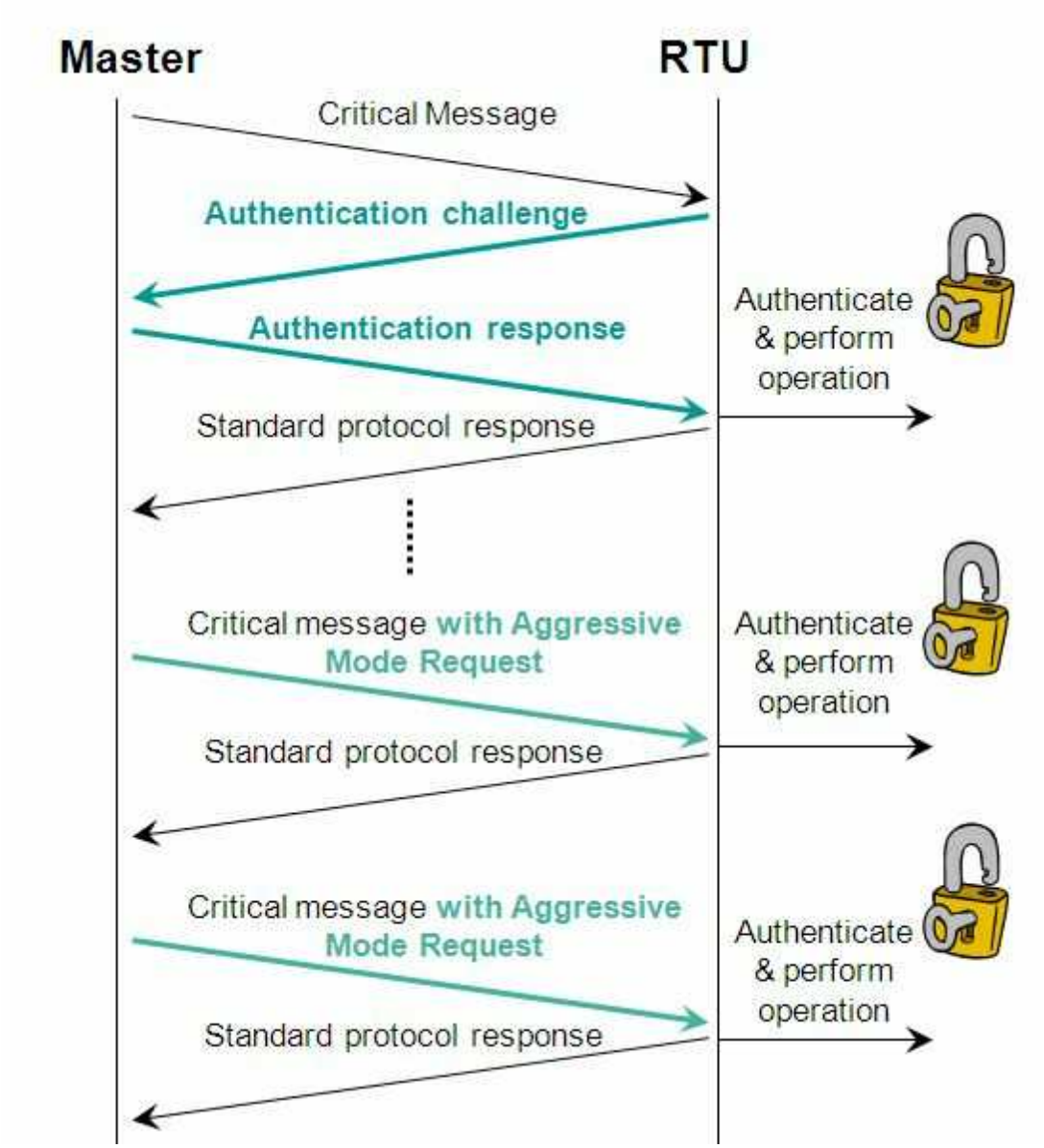
This setting affects only the RTU for which it is configured.

7.2.3 Aggressive Mode

Aggressive Mode is a security configuration, set by the Security Administrator. It is either enabled or disabled.

It allows challenge data to be appended to a critical request message without having to go through the full challenge / response exchange, as shown in the following picture. I.e. it is a more efficient short-form method of providing authentication information in critical transactions.

When enabled, Authentication mode is not used immediately. In conformance with DNP3's use of the IEC62351 13 standard, security credentials need to first be confirmed between the devices through a full authentication challenge / reply transaction. I.e. the first challenge of a critical operation uses a full authentication challenge / response transaction exchange. Subsequent critical 18 operations can then use aggressive mode.



It is equally secure to operate DNP3 Secure Authentication transactions with Aggressive Mode enabled or disabled. It is more bandwidth efficient to operate with it enabled when there are multiple controls issued in a single session.

A configuration option is provided for Aggressive Mode as a requirement of the IEC62351 13 standard.

7.2.4 Vulnerabilities Addressed

Outstation security modes can be changed remotely, for convenience, if so enabled. For highest security disable this in the SCADAPack E Security Administrator application. Security configuration then requires Physical Access.

Setting a Master Key requires Physical Access.

The RTU's general configuration file does not hold a copy of security information such as keys or security modes. Key configurations are stored in encrypted format.

When using Peer communications, security considerations are as needed as enabling secure communication with a master station. In SCADAPack E, security configurations require peer nodes to use the same Common Key (e.g. configured by using the same Security configuration file).

Remote I/O communication is not authenticated. When the RTU uses Remote I/O and is connected to a DNP3 Secure Authentication network it is recommended that the Remote I/O not use this same connection. For example:

- The Main RTU uses the ETH 1 port for connection with the DNP3 Secure Authentication network and uses ETH 2 port for Remote I/O.
- The Main RTU uses a serial for connection with the DNP3 Secure Authentication network and ETH 1 for Remote I/O.

7.3 AGA12 Encryption

There are two broad ways an RTU may be used with AGA12 encryption:

- As an AGA12-2 Node RTU
- As an AGA12 Gateway

A number of DNP3 communication port types are used when security is active on SCADAPack E RTUs. These are described in more detail throughout this Section. In summary the port types are:

- AGA12 Ciphertext ports
- One DNP3 Local Access Port
- One DNP3 Clear Device Port (AGA12 Gateway only)

- ***AGA12 Node RTU*** 45
- ***AGA12 Gateway and Session Establishment*** 47
- ***AGA12 Gateway RTU*** 49
- ***Secure Communications and Node Operation*** 52
- ***Typical System Layout*** 54
- ***Addressing and Local Communication*** 55
- ***Remote RTUs Communicating using an AGA12 Gateway*** 56
- ***Operating as a Data Concentrator*** 57
- ***Example Configurations*** 58
- ***AGA12 Parameters*** 60

7.3.1 AGA12 Node RTU

The majority of SCADAPack E RTUs in an AGA12 Encryption secured system will operate as ***AGA12 Node RTUs***. This includes RTUs whose functions are:

- End node devices communicating with Master Station(s)
- End node devices communicating with Peer node devices
- Routing devices that pass messages between RTU sub-networks:
  - AGA12-2 frame routing
  - Cleartext DNP3 frame routing (where Mixed Mode is enabled)

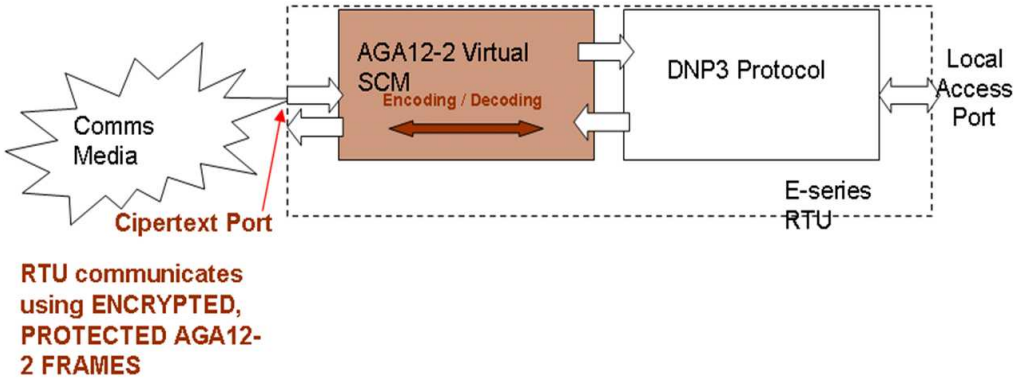


Figure 5.2: AGA12 Node as an RTU End Node Device

AGA12 Node RTUs are configured (through the SCADAPack E DNP3 Network Routing Table) with the SCM address (DNP3 destination address) of the AGA12 Gateway through which they communicate with the Master Station. The route entry's **AGA12** field needs to be set to one of the *AGA12 Gateway* settings (*AGA12 GW1*, *AGA12 GW2*, ...).
The SCM address of the Gateway is itself set through the Security Administrator software, and security configurations loaded to the AGA12 Node RTUs include configurations for up to five (5) AGA12 Gateway devices in a system. Typically the AGA12 Node RTU's gateway will be selected by choosing ***AGA12 GW1*** in the route tables AGA12 field. Check with security administration personnel if you are unsure of the configuration to use for a specific AGA12 Node RTU.

Message Routing

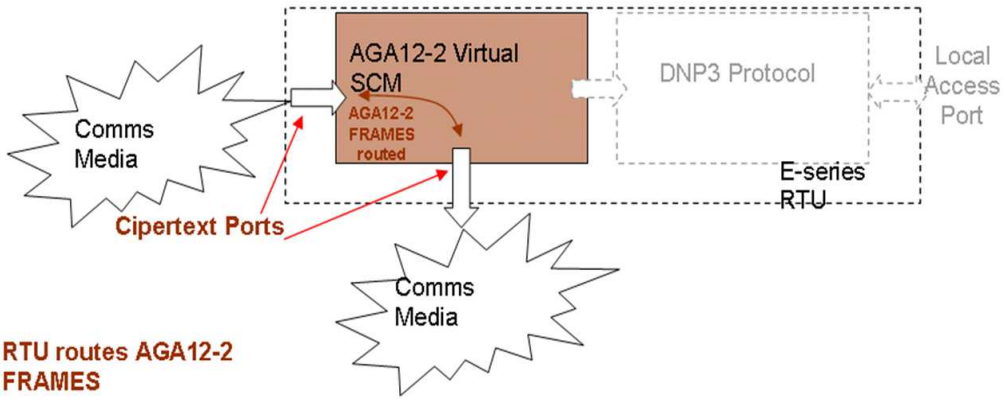


Figure 5.3: AGA12 Node as a Routing Device

Message routing is a standard feature of SCADAPack E RTUs.

AGA12 frames are routed according to the RTU's **DNP Network Routing Table** rules. When simply routing AGA12 frames, the **AGA12** setting in the route table is not used, and security Counterpart List entries are not required in the RTU.

I.e. routing AGA12 follows the same rules in the RTU as for routing of DNP3 frames.

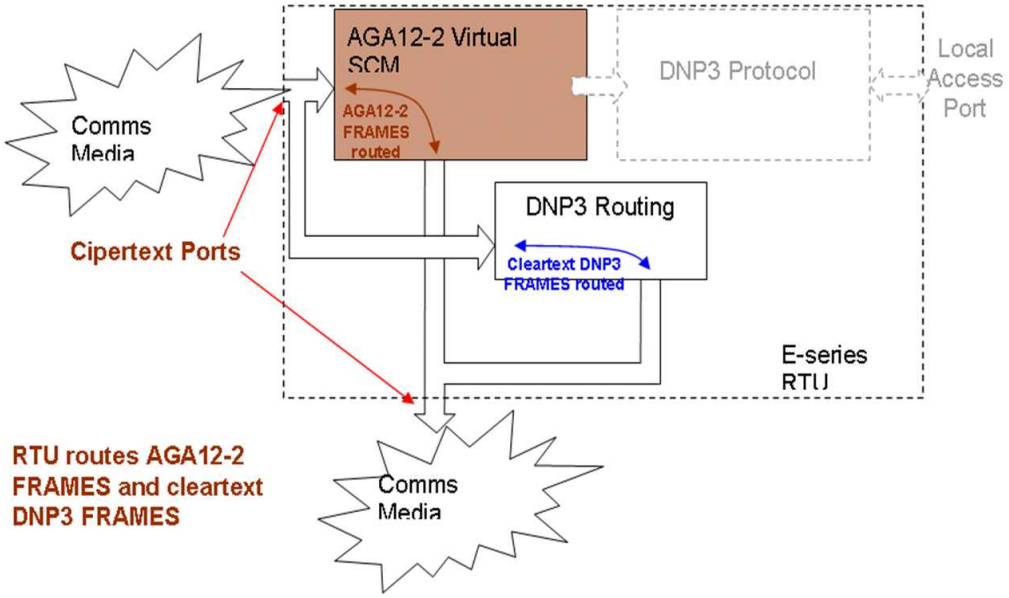


Figure 5.4: AGA12 Node as a Routing Device in Mixed Mode

Message routing is a standard feature of SCADAPack E RTUs. An AGA12 Node can route both AGA12 frames and DNP3 frames when it is operating in *MIXED MODE*.

AGA12 and DNP3 frames are routed according to the RTU's **DNP Network Routing Table** rules. When routing AGA12 and DNP3 frames, the **AGA12** setting in the route table is not required in a routing-only RTU, and security Counterpart List entries are not required in the RTU.

i.e. routing AGA12 frames follow the same rules in the RTU as for routing of DNP3 frames.

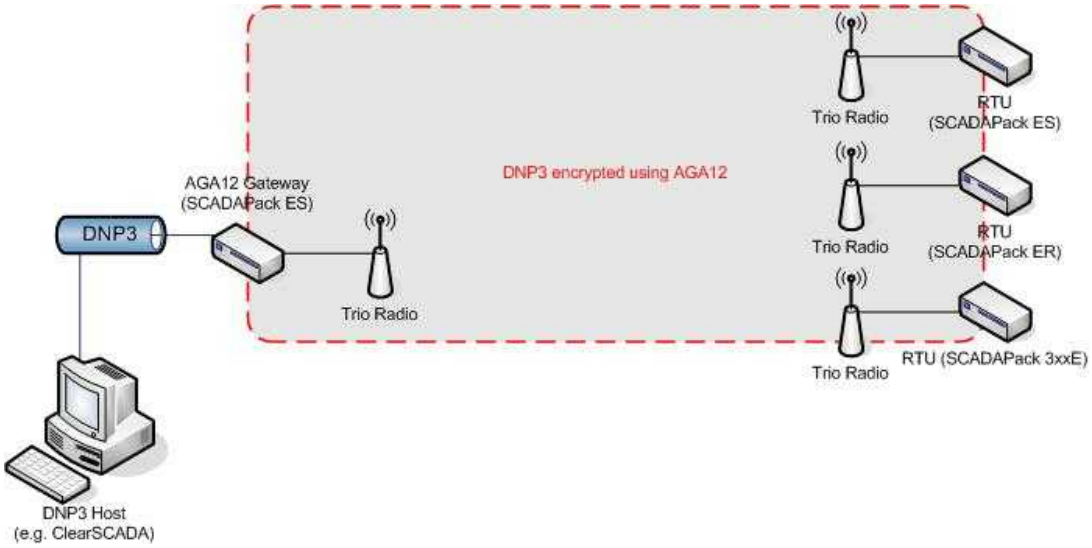
7.3.2 AGA12 Gateway and Session Establishment

AGA12 Gateway

Typically an SCM is used to take DNP3 messages received from a SCADA master on a **Clear Device Port**, encodes it, then sends the secure data out a **Ciphertext Port**. The virtual SCM on an SCADAPack E RTU configured as an *AGA12 Gateway* is used for this purpose.

It is highly recommended that a SCADAPack ES or SCADAPack ER RTU is used as an AGA12 Gateway.

The AGA12 Gateway RTU is usually installed at the host (master station), and is capable of establishing cryptographic sessions with multiple remote SCMs (SCADAPack E RTU Virtual SCMs) on the same communications link. The AGA12 Gateway RTU can also communicate with remote RTUs that not having physical or virtual SCMs installed. This is only possible when **Mixed Mode** is enabled on the AGA12 Gateway RTU. The figure below illustrates a typical installation where DNP3 is encrypted using AGA12, and uses an AGA12 Gateway:



When operating in Mixed Mode. the AGA12 Gateway RTU is configured (through the SCADAPack E DNP3 Network Routing Table) with the SCM address (DNP3 destination address) of remote devices that have protection enabled, and to which AGA12 encoded messages need to be sent. Setting the route entry's **AGA12** field to *AGA12 Node* does this.

In addition, the AGA12 Gateway is configured for DNP3 destination addresses for RTUs that do not have protection enabled, and to which cleartext DNP3 messages need to be sent. Similarly cleartext messages arriving for the Master Station from unprotected RTUs needs to be allowed through the AGA12 Gateway RTU to the Master Station. Setting the route entry's AGA12 type to *None* does this.

For more information on AGA12 Gateway configuration, see Section ***Configuring a AGA12 Gateway RTU*** 51.

Session Establishment

SCM configuration includes details for authorizing session establishment (connection) to other AGA12 devices. This authorization is managed by way of entries in a **Counterpart List** by security administration personnel using the Security Administrator.

Knowledge of DNP3 nodes, including unprotected nodes and AGA12 Gateways, is handled in the **DNP3**

Network Routing table in the same manner as standard DNP3 communication configuration. See Section ***Remote RTUs Communicating Via a AGA12 Gateway*** 56.

An SCM at the master establishes a cryptographic session with its SCM counterpart (or multiple SCM counterparts) on the channel. After a cryptographic session is established, the SCMs encrypt and authenticate SCADA messages between each other. Where a single SCM has multiple counterparts, cryptographic sessions need to be individually opened for each counterpart pair. A session is typically established between SCMs as a result of a DNP3 message that is initiated from one of the devices. A small delay is introduced while AGA12 session establishment messages are exchanged between the SCMs. Following this and while the session remains open, each DNP3 message corresponds to one AGA12 message.

The cryptographic algorithms that are used between SCM counterparts are negotiated between the SCMs ("the **Cipher Suite**") when the session is established.

Cryptographic sessions have a finite expiration based on time. After expiration, an SCM needs to establish a new session with its counterpart SCM(s) to resume secure communications.

A session can be re-established by either of the counterpart SCM(s) when there is a requirement to send a new message (payload). See ***Diagnostic Example - Session Re-establishment Transactions*** 89.

7.3.3 AGA12 Gateway RTU

AGA12 Encryption secured RTU systems may include one or more SCADAPack E ***AGA12 Gateway*** RTUs. An AGA12 Gateway RTU is a standard SCADAPack E RTU configured for AGA12 Gateway operation.

It is highly recommended that a SCADAPack ES or SCADAPack ER be used as AGA12 Gateway RTUs.

The purpose of an AGA12 Gateway is to:

1) Provide access to DNP3 Master Station(s) to a secured AGA12 system by:

- Encoding and routing cleartext DNP3 to AGA12 ciphertext
- Passing cleartext DNP3 frames from Master to remote unsecured RTUs (where *MIXED MODE* is enabled)

2) Secure the access from DNP3 remote configuration & maintenance tools to a secured AGA12 system

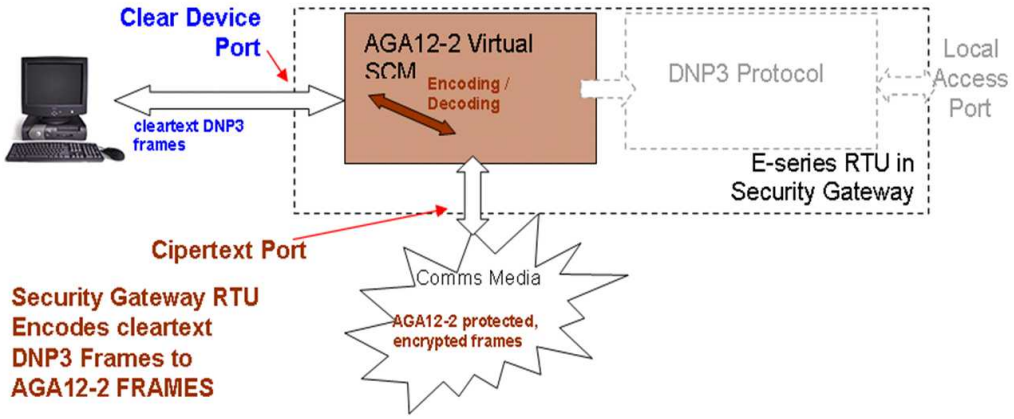


Figure 5.5: AGA12 Gateway RTU (Mixed Mode disabled)

Encoding and decoding of messages on behalf of other devices can only be done in *GATEWAY MODE*. This security mode is configured by the SCADAPack E Security Administrator application.

The AGA12 Gateway RTU needs to be physically and logically secured from external influences. The RTU's **DNP Network Routing Table** includes a Security Type identifying and authorizing encoding and decoding of messages to AGA12 protected device(s). Security COUNTERPART ENTRIES are required for each remote SCM or Virtual SCM with which the AGA12 Gateway communicates.

MIXED MODE

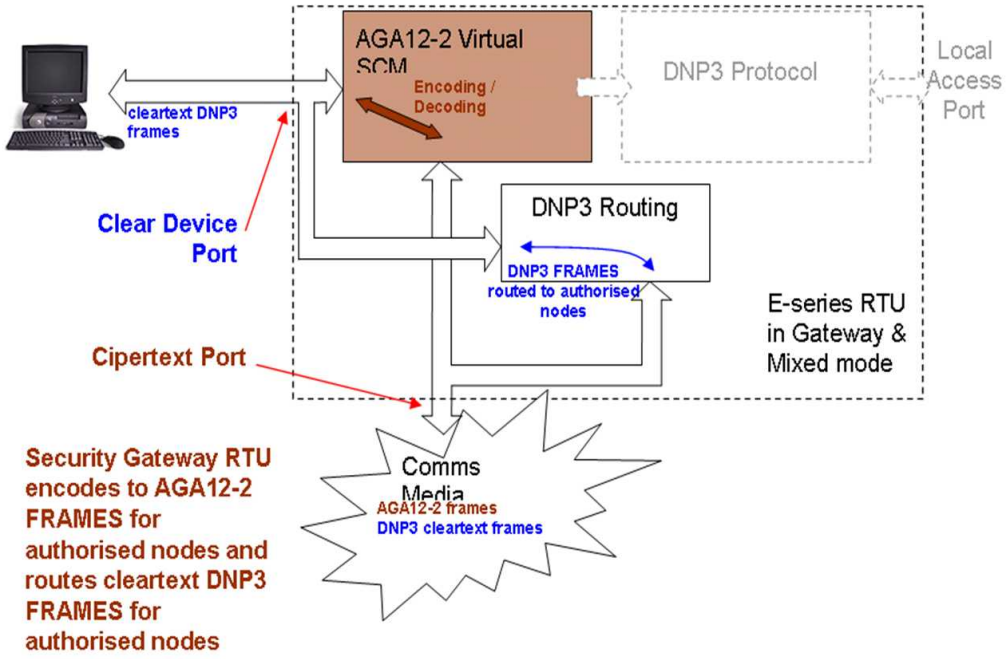

AGA12-2 Virtual SCM
Encoding / Decoding
DNP3 Protocol
Local Access Port
cleartext DNP3 frames
Clear Device Port
DNP3 Routing
DNP3 FRAMES routed to authorised nodes
E-series RTU in Gateway & Mixed mode
Cipertext Port
Security Gateway RTU encodes to AGA12-2 FRAMES for authorised nodes and routes cleartext DNP3 FRAMES for authorised nodes
Comms Media
AGA12-2 frames
DNP3 cleartext frames

Figure 5.6: AGA12 Gateway RTU Operating in Mixed Mode

Encoding and decoding of messages on behalf of other devices can only be done in *GATEWAY MODE*. The AGA12 Gateway RTU needs to be physically and logically secured from external influences. The RTU's **DNP Network Routing Table** includes a *Security Mode* identifying and authorizing encoding and decoding of messages to AGA12 protected device(s). When in MIXED MODE, the Network Routing Table also authorizes routing of cleartext DNP3 messages to DNP3 devices, from the Clear Device Port to a Ciphertext Port.

Security COUNTERPART ENTRIES are required for each AGA12 remote SCM device or Virtual SCM with which the AGA12 Gateway communicates.

Gateway mode, Mixed Mode and Counterpart Entries are configured by the SCADAPack E Security Administrator application

- ***Configuring an AGA12 Gateway RTU*** 51

7.3.3.1 Configuring an AGA12 Gateway RTU

The role of an AGA12 Gateway RTU is to take received cleartext DNP3 frames and encode the messages to ciphertext AGA12 frames. Similarly, the AGA12 Gateway takes cipertext AGA12 frames and decodes and transmits them as cleartext DNP3 frames.

Typically an AGA12 Gateway RTU is used to provide access to a secured RTU network, on behalf of a DNP3 Master Station or configuration packages not supporting AGA12 communication.

Given the primary function of an AGA12 Gateway RTU is to provide access to a secured RTU network, deployment of AGA12 Gateway RTUs needs to be carefully considered. AGA12 Gateway RTUs need to be located in a physically and logically secure environment. Typically they will be located adjacent to the master station, possibly connected via serial links. If a TCP/IP LAN or WAN network interconnects an AGA12 Gateway with a master station, the TCP/IP network needs to itself be secured. If this TCP/IP network is to be interconnected with further networks, firewalls and other security mechanisms may be required.

To configure a AGA12 Gateway, plug in the appropriate media “security key” provided by the Security Administrator or open the DNP3 Network Property page in SCADAPack E Configurator and enter the appropriate information on the DNP3 Routing table.

Typically, you configure an AGA12 Gateway RTU with a number of counterpart entries, one for each remote SCM device or Virtual SCM (RTU) with which the AGA12 Gateway communicates.

By default, a AGA12 Gateway RTU also has MIXED MODE enabled (as required by the AGA12-2 standard). This allows an AGA12 Gateway RTU to be configured to pass received cleartext DNP3 on to devices on a protected network, unmodified. This mode may be disabled for improved security at the expense of requiring ALL nodes on the network to be operating with AGA12 encryption.

7.3.4 Secure Communications and Node Operation

AGA12 Encrypted Communications

After a cryptographic session is opened between SCM devices, a message arriving at the remote SCADAPack E RTU enters the Virtual SCM from the Ciphertext Port where it is decoded (verified and decrypted) then passed to DNP3 for normal processing. When a response is generated by the RTU, the DNP3 message passes into the Virtual SCM for encoding (encrypting and signing) and is then transmitted on the Ciphertext Port.

Cleartext DNP3 messages are NOT processed on ciphertext ports.

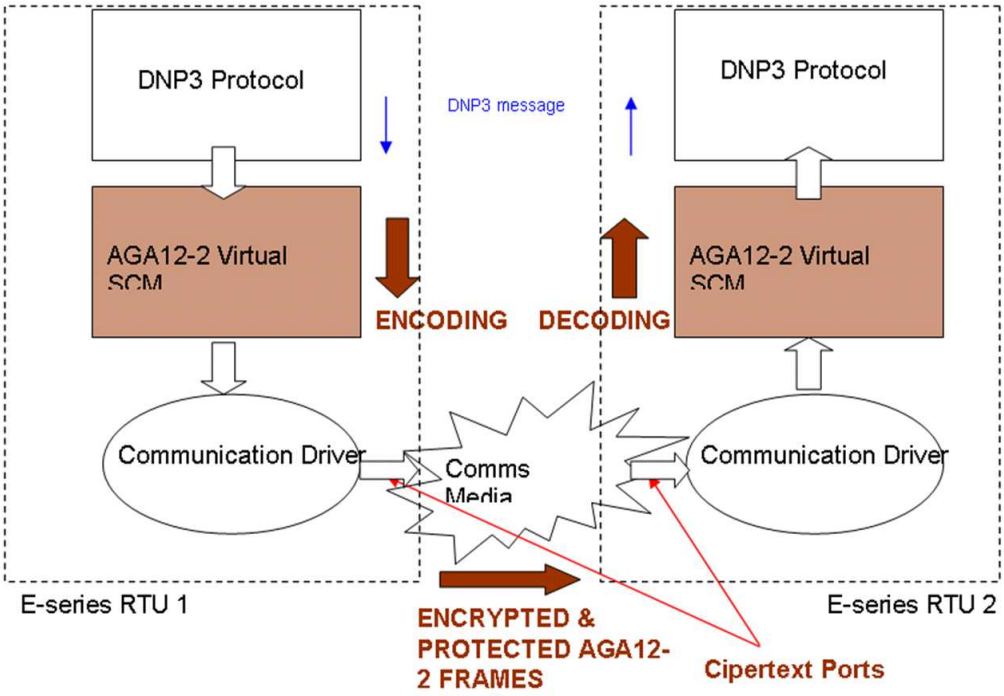


Figure 5.1: Encoding and Decoding DNP3 with AGA12

DNP3 Secure Authentication Communications

Unlike AGA12 encryption, DNP3 Secure Authentication does not use the concept of a Local Access Port on a controller nor is an AGA12 Gateway RTU required. To use DNP3 Secure Authentication, you need to have a Master that natively supports DNP3 Secure Authentication, that being, a Master Station Host or a Data Concentrator. DNP3 Secure Authentication is enabled using the same security file generated by the Security Administrator.

DNP3 Secure Authentication and AGA12 Encryption Communications

To use DNP3 Secure Authentication and AGA12 Encryption simultaneously requires a DNP3 security-capable Master and an AGA12 Gateway RTU. Using both DNP3 Secure Authentication and AGA12 Encryption modes requires configuration for security parameters for both security methods. The SCADAPack E Security Administrator provides for combined mode operation.

Secure Node Operation

On an SCADAPack E AGA12 Node RTU, all but one of the DNP3 communication ports (including

Ethernet and PPP ports) are Ciphertext ports. One port on SCADAPack E RTUs is set-aside as a Local Access DNP3 port for configuration of the RTU (as normal).

Configuration of encryption settings on an SCADAPack E RTU is not carried out through the normal configuration mechanism. You need to configure AGA12 Encryption using the Security Administrator application. Use a plug-in Compact Flash card 31 for SCADAPack ES / SCADAPack ER , or locally through the USB port from the SCADAPack E Configurator. Remotely configuring Security using SCADAPack E Configurator is also possible if configured by the Security Administrator.

Routing is supported for ciphertext AGA12 frames and cleartext DNP3 frames (when in mixed mode). For more information see ***Routing*** 65.

7.3.5 Typical System Layout

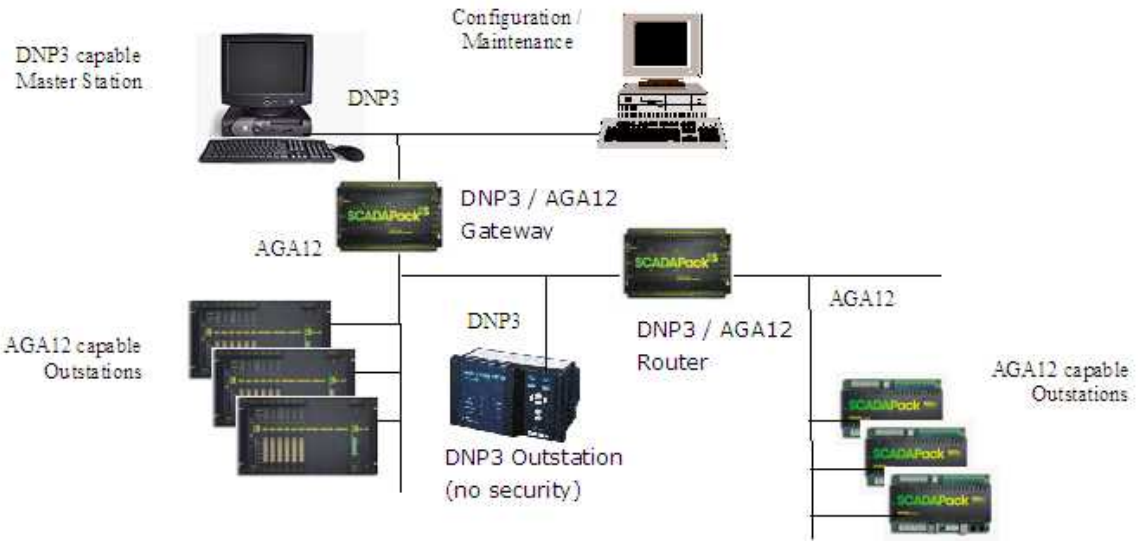


Figure 8.1: Where AGA12 Gateway is Used (example shows Mixed Mode)

7.3.6 Addressing and Local Communication

Addressing

Default DNP3 node address 0 on a new or initialized SCADAPack E RTU is not supported by AGA12 on ciphertext ports. As such, a DNP3 address change is required for an RTU before it is used as an AGA12 Encryption secured device.

Where an RTU sends data to a node (typically the master) across the AGA12 Gateway, an SCM address which differs from the DNP3 destination address is required (see Example Configurations 58). This is so that the AGA12 message is delivered to the AGA12 Gateway, it extracts the protected DNP3 message, which is then forwarded to the Master at its DNP3 address. In these cases, AGA12 nodes are configured with the SCM address of the AGA12 Gateway.

DNP3 device addresses in an interconnected system NEED TO BE UNIQUE so that the derived SCM addressing is unique.

Local Communications

When you enable AGA12 encryption on an SCADAPack E RTU device without DNP3 Secure Authentication, DNP3 communications on serial or Ethernet ports on the device are protected. that being, DNP3 ports are ciphertext ports except one single *Local Access Port* (DNP3 cleartext serial port).

A single Local Access DNP3 cleartext port is enabled on the RTU (by default, port 1) when encryption is active. Local configuration and maintenance by the SCADAPack E Configurator. routing of cleartext packets is still possible on this port (subject to mixed mode settings. This port may be changed from port 1 to another port, but to do so, this needs to be configured through a new security configuration file from the SCADAPack E Security Administrator application. When you specify a new port for Local Access operation, the previous Local Access DNP3 port automatically becomes a ciphertext protected port.

It is valid for an SCADAPack E RTU Ethernet port or serial PPP port to be chosen as the Local Access port. Using an IP capable port for this purpose needs to be considered carefully. Exposing an IP port to connections beyond the vicinity of the local RTU may invalidate the use of AGA12 as a security methodology.

7.3.7 Remote RTUs Communicating using an AGA12 Gateway

This section describes remote RTUs sending data to AGA12 Gateway nodes. See Section ***Configuring an AGA12 Gateway RTU*** 51 for a description of how to use and configure an AGA12 Gateway RTU.

Distributed DNP3 and AGA12 communication is configured in the RTU's **DNP Network Route Table**. To access the appropriate security fields in the SCADAPack E Configurator, ensure the configurator's *RTU Features* selection includes the "AGA12 Encryption" setting.

Where route table entries are added for operation as a data concentrator or peer node, an AGA12 encryption type can be set for each route entry. Typically this will be set to "AGA12 Node" for devices protected by AGA12 and therefore communicating using ciphertext.

Where the route directs messages using an AGA12 gateway node, select from one of the "AGA12 GWn" types on the route entry. This causes the AGA12 messages to be directed to a nominated gateway SCM address rather than to the destination DNP3 address. A route entry for a master station needs to be present where an AGA12 Gateway is used for communication with that master station.

An "AGA12 GWn" type can select from one of five Gateway SCM (DNP) addresses. Multiple gateways can be used for a number of purposes including multiple masters and distributed access from configuration terminals. See Section ***Peer Communication, Multiple Masters, & Start-Up and Shutdown*** 67 **(Multiple Masters)** 67.

The Gateway SCM addresses form part of the security configuration set by the Security Administrator. Security Configuration is deployed via plug-in media (SCADAPack ES / SCADAPack ER) or via SCADAPack E Configurator.

When sending a DNP3 message using AGA12 ciphertext (e.g.. encoding a DNP3 frame to AGA12) and there is a route entry selecting an "AGA12 GWn" type for that entry, the AGA12 frame is sent to the nominated device (Virtual SCM) address, rather than the device at the destination DNP3 address. The destination DNP address, being transported by the AGA12 frame, is not modified.

For DNP3 frames to be sent to a Master in ciphertext, and for which no route entry is present for the master's DNP3 address, the master's DNP3 address will be used as the destination SCM address (this is the default).

For systems using an AGA12 gateway, each remote AGA12 secured RTU requires an "AGA GWn" type to be set in the* DNP3 Network Route Table. *You need also configure a Gateway SCM address..

7.3.8 Operating as a Data Concentrator

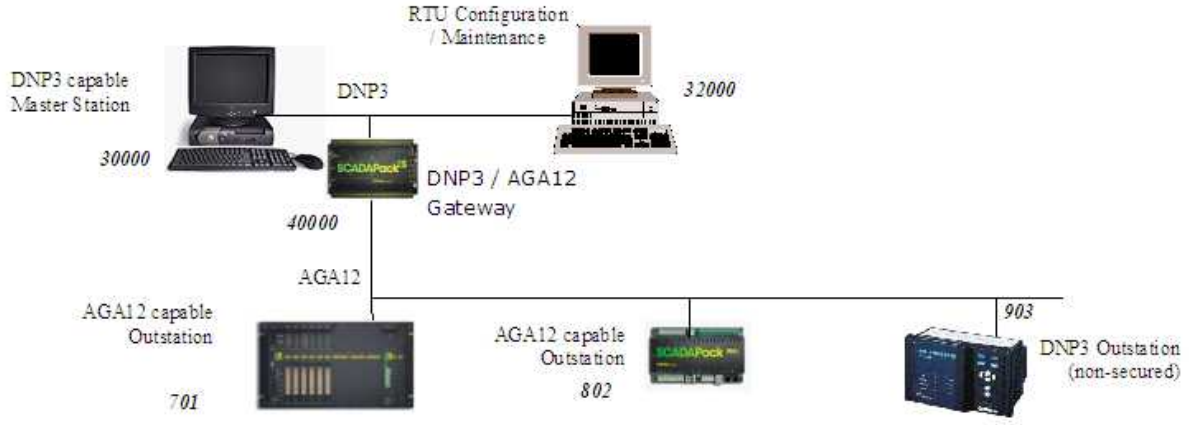
When licensed with a DNP3 Master (data concentrator) functionality, DNP3 ports may need to communicate with cleartext 9 DNP3 slave devices and possibly ciphertext devices, on the same port.

The following will apply if AGA12 encryption is enabled on a Data Concentrator RTU:

- DNP3 ports operate as AGA12 encrypted ciphertext 9 ports.
- The AGA12 column shows each remote RTU node (or node range) route entry as *NONE* (cleartext DNP3 device with no encryption - default) or *AGA12 Node* device (secured DNP3).
- Nodes defined as AGA12 devices will also require counterpart list entries.
- Normal data concentrator DNP3 processing and routing rules apply
- Cleartext DNP3 can be sent and received by the data concentrator on an AGA12 protected port only if the RTU is configured for operation in Mixed Mode 10.

7.3.9 Example Configurations

Communication required between master station 30000 and RTU nodes through an AGA12 Gateway, RTU Configuration / Maintenance computer permitted to connect to nodes 701 and 802, and peer communications required between 701 and 802.



1. Simply plug in a media 'Security Key' (e.g. CompactFlash card) from your Security Administrator into each SCADAPack ES or SCADAPack ER RTU in turn and setup the routing tables as below For SCADAPack 300E RTUs load the security file via USB using SCADAPack E Configurator. Alternatively,
2. **Setup configurations as follows:**

RTU 701 configurations:

Common Key 123456789ABCDEF0123456789ABCDEF0
Mac Key ABCDEF0123456789ABCDEF0123456789ABCDEF01
Gateway 1 SCM Address 40000
Counterpart List: 701, 802

As a AGA12 Gateway RTU (address 40000) is used for master and SCADAPack E access, routing entries with SCM addressing will be required:

Src Port	Src Start	Src End	Dest Start	Dest End	Dest Port	Connect Number	AGA12	Status ...
Any	0	65535	30000	30000	Port 2		AGA GW1	
Any	0	65535	802	802	Port 2		AGA12 Node	

RTU 802 configurations:

Same Group security configuration as 701.

As a AGA12 Gateway RTU (address 40000) is used for master and SCADAPack E Configurator access, routing entries with SCM addressing will be required:

Src Port	Src Start	Src End	Dest Start	Dest End	Dest Port	Connect Number	AGA12
Any	0	65535	30000	30000	Port 2		AGA GW1
Any	0	65535	701	701	Port 2		AGA12 Node

RTU 903 configurations: AGA12 security not supported, so standard configurations only

Gateway 40000 configurations:

GATEWAY mode: enabled

MIXED MODE: enabled

Clear Device Port: ETH1

Common Key 123456789ABCDEF0123456789ABCDEF0

Mac Key ABCDEF0123456789ABCDEF0123456789ABCDEF01

Src Port	Src Start	Src End	Dest Start	Dest End	Dest Port	Connect Number	AGA12
Ethernet 1	30000	30000	701	899	Port 2		AGA12 node
Ethernet 1	30000	30000	901	999	Port 2		NONE
Port 2	701	999	30000	30000	Ethernet 1	1.2.3.4:U	NONE

This entry with AGA12 security will use the Destination DNP address as the SCM address, thereby minimizing configuration in the route table, and maximizing use of route range entries.

The gateway RTU's route entry 901-999 sends data to Cipher-text port 2, but in cleartext mode (i.e. no security). This is Mixed Mode communications.

7.3.10 AGA12 Parameters

The following sections describe parameters associated with AGA12-2 serial protocol (known as SSPP), their pre-defined use for DNP3 operation (as per AGA12-2 reference code) and SCADAPack E RTU user configured parameters:

- ***DNP3 Routing Table and AGA12 Settings*** 61
- ***Fixed AGA12-2 Parameters*** 63
- ***Vulnerabilities Addressed*** 64

7.3.10.1 DNP3 Routing Table and AGA12 Settings

Route Table

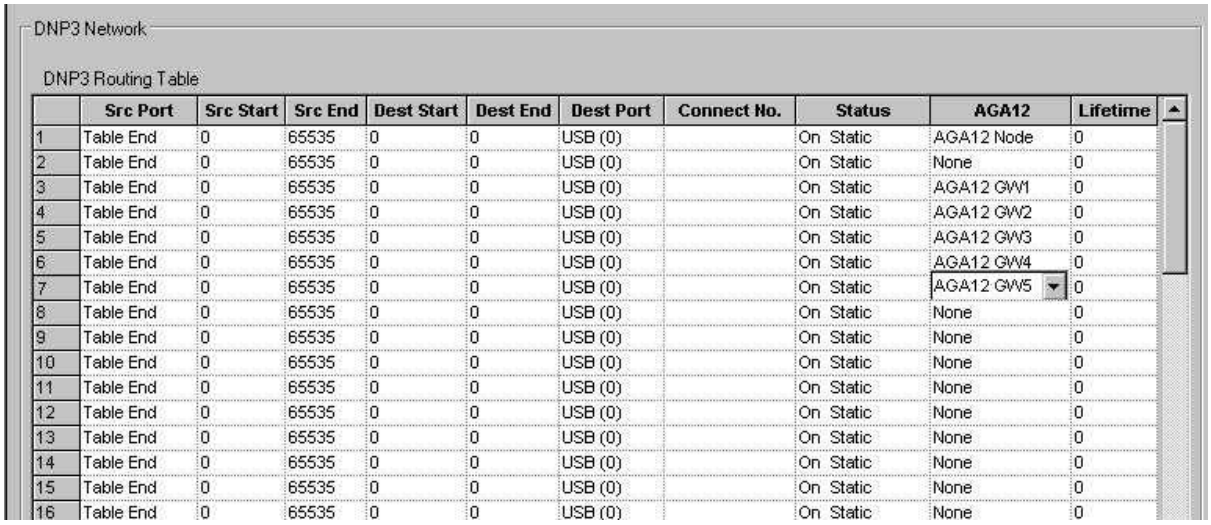
A AGA12 Gateway requires knowledge of nodes whose packets (received on the clear device port) are going to be encrypted and sent to a cipher port. An AGA12 Gateway also requires knowledge of cleartext nodes whose packets are to be routed and sent in the clear (when in MIXED MODE). It derives this information from the routing table.

The Routing table AGA12 type selections include:

- None (default)
- AGA12 Node
- AGA12 GWn

A gateway will generally use AGA12 Node for route entries to RTU devices supporting encryption, and None for route entries to conventional devices using standard DNP3 communications.

AGA12 GWn types are not usually used in configurations on a gateway. Typically they are used for end-node RTUs.


DNP3 Network

DNP3 Routing Table

	Src Port	Src Start	Src End	Dest Start	Dest End	Dest Port	Connect No.	Status	AGA12	Lifetime
1	Table End	0	65535	0	0	USB (0)		On Static	AGA12 Node	0
2	Table End	0	65535	0	0	USB (0)		On Static	None	0
3	Table End	0	65535	0	0	USB (0)		On Static	AGA12 GW1	0
4	Table End	0	65535	0	0	USB (0)		On Static	AGA12 GW2	0
5	Table End	0	65535	0	0	USB (0)		On Static	AGA12 GW3	0
6	Table End	0	65535	0	0	USB (0)		On Static	AGA12 GW4	0
7	Table End	0	65535	0	0	USB (0)		On Static	AGA12 GW5	0
8	Table End	0	65535	0	0	USB (0)		On Static	None	0
9	Table End	0	65535	0	0	USB (0)		On Static	None	0
10	Table End	0	65535	0	0	USB (0)		On Static	None	0
11	Table End	0	65535	0	0	USB (0)		On Static	None	0
12	Table End	0	65535	0	0	USB (0)		On Static	None	0
13	Table End	0	65535	0	0	USB (0)		On Static	None	0
14	Table End	0	65535	0	0	USB (0)		On Static	None	0
15	Table End	0	65535	0	0	USB (0)		On Static	None	0
16	Table End	0	65535	0	0	USB (0)		On Static	None	0

Encryption Settings

AGA12 encryption settings for an AGA12 Gateway operate the same way as a remote RTU. Encryption modes and counterpart entries are configured by the Security Administrator application and deployed through Compact Flash “security key” (SCADAPack ES / SCADAPack ER) or SCADAPack E Configurator. Configuration of gateway settings for non-secured and secured nodes is via a combination of settings in the **DNP3 Network Routing Table** (AGA12 type field) and AGA12 counterpart entries. Nodes that have entries in the routing able with AGA12 selection also require an entry in the counterpart list. AGA12 frames can also be routed.

Remote RTUs prevent encoding of cleartext DNP3 on a ciphertext link by not allowing gateway functions. On an AGA12 Gateway RTU, high levels of protection can only be provided by secure environments on the AGA12 Gateway and strict source/destination routing.

In-bound (serial) DNP3 requests for the gateway node address (e.g., remote access attempts to the gateway configuration) need to be authorized through AGA12. This means the remote access attempt needs to have a matching key and have a valid session connected.

7.3.10.2 Fixed AGA12-2 Parameters

The following AGA12-2 SSPP (Serial SCADA Protection Protocol) options are used by SCADAPack E RTUs. Refer to the *AGA12 Standard* for more information.

- SSPP 8-bit Link Layer only
- No Broadcast frames
- No Management sessions support (future)
- Encryption algorithm: AES128CTR (fixed)
- CipherSuite: HmacSHA1 (fixed)
- SCM address = RTU DNP3 node address
- SSPP Link Layer Markers for DNP3 are as follows (from AGA12-2 DNP3 reference code):

Link Layer Marker	Control Octet (hex)
ESC	10
SOM	11
SOT	13
EOM	14

- Replacement Characters are byte stuffed in the SSPP data stream. For SCADAPack E RTU security implementation, these are chosen to minimize cleartext DNP3 frames from attempting synchronization part way through a ciphertext SSPP frame. SCn characters represent the SCADA protocol Character to be replaced. RCn characters represent the replacement Character. Hardcoded characters are chosen as follows:

SC1	05
RC1	15

ESC octets are byte stuffed with ESC ESC if followed by one of ESC, SOM, SOT, EOM, SC1, RC1.

For SCADAPack E RTUs, 05 octets are replaced by 10 15

A Typical SSPP frame format:

ESC SOM 10-byte-header encrypted-payload **ESC SOT** trailer **ESC EOM**

10 11 header… payload… **10 13** trailer… **10 14**

7.3.10.3 Vulnerabilities Addressed

Outstation security modes can be changed remotely, for convenience, if so enabled. For highest security disable this in the SCADAPack E Security Administrator application. Security configuration then requires Physical Access.

Setting a Master Key requires Physical Access.

Routing and encoding from cleartext to ciphertext is only permitted in AGA12 Gateway mode.

The state of the Gateway mode setting can be read via a read-only system point, but cannot be changed remotely or using SCADAPack E Configurator (default is Gateway Mode DISABLED).

The RTU's general configuration file does not hold a copy of security information such as keys or security modes. Key configurations are stored in encrypted format.

AGA12 Mixed Mode operation (processing messages for both cleartext and ciphertext on the same port) is permitted for routing and on an AGA12 Gateway mode. It operates in conjunction with routing entries. Mixed mode operation on RTUs relates to cleartext DNP3 routing on ports. A system point indicates if mixed-mode is enabled or disabled. If enabled, may be disabled remotely. If mixed-mode is enabled, cleartext and ciphertext routing is permitted on Cipher-text ports on all nodes – it is the responsibility of the end-node to protect itself.

When using Peer communications, security considerations are as necessary as enabling secure communication with a master station. In SCADAPack E, security configurations require peer nodes to use the same Common Key (e.g. configured by using the same Security configuration file).

7.4 DNP3 Routing

DNP3 Secure Authentication

When DNP3 Secure Authentication is enabled, a routing mechanism that uses a variable address structure creates a routing path between communicating devices. The routing path reduces protocol overhead typically associated with network layers and provides a unique network address for every device in the distribution system. The routing mechanism is interoperable with DNP3- based devices and does not alter the DNP3 specification.

Routing in an AGA12 Network

Routing can be used for SCADAPack E outstation network architectures supporting cleartext DNP3, ciphertext AGA12, and mixed systems. Provision of encyrption and authentication to these SCADAPack E architectures requires routing facilities to be secured. Typically, only a few DNP3 nodes (devices) in a DNP3 network are configured to route DNP3 traffic. These devices usually have two or more DNP3 communication ports and are are used to connect sub-networks (groups) of RTUs together.

AGA12 Message Encryption

When AGA12 message encryption is enabled, typical SCADAPack E outstation DNP3 network architectures are retained, (for example, radio repeater or sub-network links), while increasing the security of such distributed systems.

An SCADAPack E outstation routes encrypted frames between ciphertext ports, intact. This improves transaction efficiency AGA12 frames which are not decoded and re-encoded before they are passed on. Counterpart entries are not required. **DNP Network Routing Table** *AGA12* type fields are not need for routing of AGA12 frames between ciphertext ports.

In accordance with AGA12-2 requirements, the SCADAPack E RTU architecture also allows mixed cleartext and protected sub-networks. You need to understand which sub-networks or individual devices are using AGA12 encryption and which are not. MIXED MODE needs to be enabled for an SCADAPack E RTU to route cleartext message to a ciphertext port.

Routing rules include:

- Protected AGA12 ciphertext frames can be routed from port-to-port when AGA12 encryption is enabled on any SCADAPack E RTU. The protected frames are untouched by the router, relying on the destination node to protect itself.
- Mixed Mode is enabled by default (following AGA12-2 standard), allowing unprotected cleartext DNP3 frames to be routed untouched (it is the responsibility of the destination node to protect itself by rejecting unprotected cleartext DNP3 frames, if necessary). If you disable Mixed Mode, cleartext DNP3 frames are not routed.
- Cleartext DNP3 frames received on a Local Access port can be routed to a ciphertext port, but only when Mixed Mode is enabled for AGA12 Encryption (only) licensing. If you have DNP3 Secure Authentication licensed, or DNP3 Secure Authentication with AGA12 Encryption as your license options, this does not apply (i.e. whenever DNP3 Secure Authentication is enabled, routing is allowed).
- Cleartext DNP3 received by a secure RTU will not be encrypted and routed in ciphertext. This is the purpose of AGA12 Gateway RTU devices, but this mode needs to be explicitly configured. This forms part of the secure configuration methodology used to configure AGA12 RTU encryption and is not permitted to be remotely enabled or disabled.
- These routing rules are supported by a number of SCADAPack E RTU diagnostics, detailing specific forwarding or rejection of frames dependent on frame type (cleartext / ciphertext), port type (ciphertext, clear device, local access), security operation (AGA12 enabled, mixed mode, gateway

mode), route AGA12 mode (None, AGA12 Node, AGA12 Gateway n). The AGA12 field defines a protocol (SSPP) for use for connecting, transporting, encrypting, and signing serial SCADA protocols including DNP3. The following selections are available:

—None (standard DNP3 device with no encryption)

—AGA12 Node (secure DNP3 device with encryption)

—AGA12 GWn (AGA12 messages are directed to a nominated gateway SCM address rather than to the DNP3 address)

Diagnostics are described further in ***System Points*** 91 including a detailed list of routing diagnostic rules.

To enable or disable Mixed Mode operation, plug in the appropriate media module set up by the Security Administrator.

7.5 Peer Communication, Multiple Masters, & Start-Up and Shutdown

Peer Communication

Where a node is protected by AGA12 encryption or DNP3 secure authentication, a peer node communicating with that node needs to use the same. With AGA12, matching counterpart entries (including key-pairs) needs to be configured for the peer device, in both devices.

Peer devices need to be configured with the security Group's Common Key 9. For AGA12, individual counterpart entries are still required listing the address for each peer node.

Multiple Masters

As the Common Key 9 is shared across a Group of devices and individual AGA12 sessions are opened with each master, the Common Key is used to authenticate each session with each master (and other devices if required).

Individual Counterpart entries are still required for AGA12 configurations.

The AGA12 Gateway address configurations previously described, also allow the use of separate AGA12 gateways for multiple masters that communicate with an SCADAPack E RTU. The AGA12 Gateway address fields may also be referenced from other routing table entries. See ***Remote RTUs Communicating Via a AGA12 Gateway*** 56.

Start-Up and Shutdown

As per the AGA12-2 standard, system start-up generates new random seeds for the OPN association number.

Upon a DNP Warm Restart or RTU Orderly shutdown, an AGA12-2 CLS (close session) is issued to any open AGA12 connections.

7.6 Security Considerations

Use of IP facilities

While the AGA12 encryption mechanism on SCADAPack E RTUs applies to media and transports used for DNP3, non-DNP3 IP application communications in particular may not be secure. As such, an RTU operating with wide area TCP/IP communications and using AGA12 encryption for DNP3 should NOT have the following services enabled without consideration of the security implications:

- Telnet
- FTP
- Modbus/TCP Server

IP Forwarding Restricted

When AGA12 Encryption security is active on an RTU operating as an AGA12 Gateway, IP Forwarding across IP interfaces (which are normally enabled on SCADAPack E RTUs) are DISABLED. This prevents one IP network interface automatically forwarding (routing) IP packets to other interfaces.

For example, in a dual Ethernet architecture, IP packets from one Ethernet interface are blocked from routing to the other Ethernet interface. A similar philosophy applies to serial PPP links and mixed Ethernet / PPP links.

Security is maintained in situations such as an AGA12 Gateway where one Ethernet interface is configured as a Clear Device port (default), and the other Ethernet interface is used as a ciphertext AGA12 secured network port.

SSPP Timing Summary

AGA12-2 includes a time-based security definition, with tolerance to aid in detecting replay attacks. Each Cipher-text frame includes a Sequence Number that is the time in ticks since the start of a session. The duration of a ‘tick’ is negotiable at OPN time (resolution in uS). For maximum security, one message fits in 1 tick.

The receiver only pays heed to a packet received where the sequence number is within a tolerance of a locally derived sequence number. If sequence numbers are incorrect, communications can’t be regained until the session expiry timer expires! A CLS (close) is sent after this time, and a new OPN restarts the sequence numbers. [Time drift tolerance also dictates a time at which this CLS/OPN process occurs normally]. Similarly the ACKTIMEOUT is used in the calculation as a measure of expected link delay to calculate the time tolerance.

8 Security Administration

Administration of the SCADAPack E RTUs security facilities is provided through the SCADAPack E Security Administrator application. This is a secure application, requiring licensed authorization to operate. To obtain an activation license for the Security Administrator, please contact Schneider Electric.

This application allows configuration of the security modes, keys, DNP3 Secure Authentication parameters, users, configurators, AGA12 Counterpart authorization and Gateway addresses, etc. It provides a Windows® user interface, and includes both manual and automatic generation of keys.

New Project - Security Administrator
File
Insert
Master Key
Help
Project
Groups
NorthernRTUs
Users
Joe
Fred
Configurators
Maint Laptop 1
Security Administrator
CONTROL MICROSYSTEMS
SCADAPack
SCADAPack S
Security Mode
AGA12-2 Encryption
DNP3 Secure Authentication
DNP3 Secure Authentication and AGA12-2 Encryption
Configurator Key Mode
Default Key
All instances of E-Series Configurator will use the same pre-shared key for DNP3 security. This is a basic form of security that does not require keys to be managed for every instance of E-Series Configurator. (Security Level: Lowest)
Common Key
All instances of E-Series Configurator will use the same key as specified below. The same security file must be imported into every instance of E-Series Configurator. (Security Level: Medium)
Common Key (Last 4 digits)
2B0B
New Key
Unique Keys
Every instance of E-Series Configurator will use a different security file. This is the most secure option but requires more security files to be managed. (Security Level: Highest)
Users Mode
No user authentication provided by the Controllers.
Individual users can be configured and authenticated by the Controllers.

Figure 9.1: SCADAPack E Security Administrator Application

8.1 Security File Management & Counterpart Entry Management

Security File Management

The SCADAPack E Security Administrator application manages security configuration files, allowing security configuration files to be exported, including to plug-in media “security key” devices for example, a Compact Flash card. This allows deployment of security configurations to the SCADAPack E RTU. Existing security configuration files can also be opened and managed.

Key values may be copied from the application to other applications. This includes SCADA Host (Master Stations) that support security keys, for example.

Common Key and security mode configurations for each RTU security *Group* are exported from the Security Administrator. It stores the security configuration for one group, or all groups in a “SYSTEM.RTK” files. This contains security configuration for both DNP3 Secure Authentication and AGA12 Encryption.

Master Key configuration for all controllers can be exported from the Security Administrator and saved as a "SYSTEM.KEY" file. The Master Key files are typically set once in the lifetime of a system, and must be deployed locally.

AGA12 Counterpart Entry Management

Authorization for this node to communicate with other AGA12 nodes is given through Counterpart Entries (including the Master Station or AGA12 Gateway RTUs). The list shown in the lower part of the Security Administrator form provides counterpart entry configuration. A separate counterpart entry is required for each node with the Group to which RTUs may communicate with.

See *SCADAPack E Security Administrator User Guide* for more information on setting Counterpart Entries.

9 Diagnostics

- ***Diagnostic Filtering*** 77
- ***Routing Rule Diagnostics*** 78
- ***Diagnostic Example - Session Open Transactions*** 82
- ***Diagnostic Example - Session Re-establishment Transactions*** 89
- ***System Points*** 91

9.1 DNP3 Secure Authentication Diagnostics

A Command line diagnostic interface is provided on the SCADAPack E RTU for DNP3 Secure Authentication. For more information on command line operation and diagnostics, refer to the *SCADAPack E Operational Reference Manual*.

Set DNP3 Diag Filters.

Usage: DNPDIAG mode filter [filter...]
Where: mode = ENABLE DISABLE
Where: filter = SECURITY ...

Other DNP3 protocol diagnostic filters are described in *SCADAPack E Operational Reference* manual.

Set the diagnostic filters on other protocol layers using DNPDIAG if necessary, then use DIAG command to enter diagnostic stream mode.

- ***Diagnostic Example - No RTU Security Configured*** 71
- ***Diagnostic Example - Incorrect Security Credentials*** 73
- ***Diagnostic Example - Successful Critical Message Challenge*** 75

9.1.1 Diagnostic Example - No RTU Security Configured

DNP3 Secure Authentication Example 1:

In the following example, a master device tries to establish DNP3 Secure Authentication session with SCADAPack E RTU.
RTU is not configured for, or does not support DNP3 Secure Authentication.

```
C:\> DNPDIAG /?
Set DNP Diag Filters.
Usage: DNPDIAG mode filter [filter ....] [param]
Where: mode   = ENABLE DISABLE
Where: filter = * 1 2 3  ETH
                APPL BYTES DBASE EVENTS FILTER_ADDR LINK NETWORK RAW_NET
SECURITY TIME TRANSP USER
DNP Diags: --- link, *** net, ~~~ trans, === appl, +++ user

C:\> DNPDIAG ENABLE APPL DBASE USER SECURITY
DNP3 Diags Enabled: 0 1 2 3 4 ETH1 APPL DBASE USER SECURITY

C:\> DIAG

Connecting to diagnostic display. Use <ESC> to disconnect

 ===> [32000]    Application Header, Authentication Request
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 1

                Rx Object 120(Authentication), variation 4, qualifier 0x07
(8 Bit Limited Quantity)
                     Rx Authentication Key Status Request, User = 1
```

```
 <+++ [32000]    Insert request in queue: NULL Response
 <=== [32000]    Application Header, Response
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 1 IIN(0x0100)

 <=== [32000]    IIN Bits:
                IIN2.0 Function Code Not Implemented

Disconnected from diagnostic display

C:\>
```

9.1.2 Diagnostic Example - Incorrect Security Credentials

DNP3 Secure Authentication Example 2:

Master device tries to establish DNP3 Secure Authentication with incorrect security credentials (separate for wrong keys vs. invalid username / password ??)

```
C:\> DNPDIAG /?
Set DNP Diag Filters.
Usage: DNPDIAG mode filter [filter ....] [param]
Where: mode   = ENABLE DISABLE
Where: filter = * 1 2 3  ETH
                APPL BYTES DBASE EVENTS FILTER_ADDR LINK NETWORK RAW_NET
SECURITY TIME TRANSP USER
DNP Diags: --- link, *** net, ~~~ trans, === appl, +++ user

C:\> DNPDIAG ENABLE APPL DBASE USER SECURITY
DNP3 Diags Enabled: 0 1 2 3 4 ETH1 APPL DBASE USER SECURITY

C:\> DIAG

Connecting to diagnostic display. Use <ESC> to disconnect

===> [32000]    Application Header, Authentication Request
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 1

                Rx Object 120(Authentication), variation 4, qualifier 0x07
(8 Bit Limited Quantity)
                     Rx Authentication Key Status Request, User = 1

<+++ [32000]    Build DNP3 Message: Authentication Key Status

                Tx Object 120(Authentication), variation 5, qualifier 0x5b
(16 Bit Free Format)
                     Tx Authentication Key Status, User = 1, Sequence = 1,
KeyWrapAlgorithm = AES 128, hmacAlgorithm = SHA1 4 OCTET, Status 2-NOTINIT

<+++ [32000]    Insert request in queue: Authentication Key Status

<=== [32000]    Application Header, Authentication Response
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 1

===> [32000]    Application Header, Authentication Request
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 2

                Rx Object 120(Authentication), variation 6, qualifier 0x5b
(16 Bit Free Format)
**** [32000]   Secure Authentication Session Key failure, length 152
expected 81****
                     Rx Authentication Key Change Request, User = 1, Key
Length = 0, Sequence = 1,  Expected = 1 FAILURE

<+++ [32000]    Build DNP3 Message: Authentication Key Status
```

```
                Tx Object 120(Authentication), variation 5, qualifier 0x5b
(16 Bit Free Format)
                     Tx Authentication Key Status, User = 1, Sequence = 2,
KeyWrapAlgorithm = AES 128, hmacAlgorithm = SHA1 4 OCTET, Status 4-AUTHFAIL

<=== [32000]    Application Header, Authentication Response
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 6
```

9.1.3 Diagnostic Example - Successful Critical Message Challenge

DNP3 Secure Authentication Example 3:

Master device establishes session, with security authentication, successfully.
Critical operations are challenged and accepted.

```
C:\> DNPDIAG /?
Set DNP Diag Filters.
Usage: DNPDIAG mode filter [filter ....] [param]
Where: mode   = ENABLE DISABLE
Where: filter = * 1 2 3  ETH
                APPL BYTES DBASE EVENTS FILTER_ADDR LINK NETWORK RAW_NET
SECURITY TIME TRANSP USER
DNP Diags: --- link, *** net, ~~~ trans, === appl, +++ user

C:\> DNPDIAG ENABLE APPL DBASE USER SECURITY
DNP3 Diags Enabled: 0 1 2 3 4 ETH1 APPL DBASE USER SECURITY

C:\> DIAG

Connecting to diagnostic display. Use <ESC> to disconnect

===> [32000]    Application Header, Authentication Request
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 1

                Rx Object 120(Authentication), variation 4, qualifier 0x07
(8 Bit Limited Quantity)
                     Rx Authentication Key Status Request, User = 1

<+++ [32000]    Build DNP3 Message: Authentication Key Status

                Tx Object 120(Authentication), variation 5, qualifier 0x5b
(16 Bit Free Format)
                     Tx Authentication Key Status, User = 1, Sequence = 1,
KeyWrapAlgorithm = AES 128, hmacAlgorithm = SHA1 4 OCTET, Status 2-NOTINIT

<+++ [32000]    Insert request in queue: Authentication Key Status

<=== [32000]    Application Header, Authentication Response
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 1

===> [32000]    Application Header, Authentication Request
                FIR(1) FIN(1) CON(0) UNS(0) SEQ# 2

                Rx Object 120(Authentication), variation 6, qualifier 0x5b
(16 Bit Free Format)
                     Rx Authentication Key Change Request, User = 1, Key
Length = 32, Sequence = 1,  Expected = 1 SUCCESS

<+++ [32000]    Build DNP3 Message: Authentication Key Status

                Tx Object 120(Authentication), variation 5, qualifier 0x5b
```

(16 Bit Free Format)
Tx Authentication Key Status, User = 1, Sequence = 2, KeyWrapAlgorithm = AES 128, hmacAlgorithm = SHA1 4 OCTET, **Status 1-OK**

<+++ [32000] Insert request in queue: Authentication Key Status

<=== [32000] Application Header, Authentication Response
FIR(1) FIN(1) CON(0) UNS(0) SEQ# 2

===> [32000] Application Header, **Direct Operate**
FIR(1) FIN(1) CON(0) UNS(0) SEQ# 3

<+++ [32000] Build DNP3 Message: Authentication Challenge

Tx Object 120(Authentication), variation 1, qualifier 0x5b (16 Bit Free Format)
Tx Authentication Challenge, User = 0, Sequence = 1, Algorithm = 1-SHA1 4 OCTET, Reason 1-CRITICAL

<+++ [32000] Insert request in queue: Authentication Challenge

<=== [32000] Application Header, Authentication Response
FIR(1) FIN(1) CON(0) UNS(0) SEQ# 3

===> [32000] Application Header, Authentication Request
FIR(1) FIN(1) CON(0) UNS(0) SEQ# 3

Rx Object 120(Authentication), variation 2, qualifier 0x5b (16 Bit Free Format)
Rx Authentication Reply, User = 1, Sequence = 1 SUCCESS

Rx Object 12(Control Relay Output Block), variation 1, qualifier 0x28(16 Bit Index)
Control Relay Output Block 000001 = 0x04(LATCH_OFF: : :NUL)
count = 1, on = 0, off = 0, status = 0(SUCCESS)

<+++ [32000] Insert request in queue: **Direct Operate Response**

<=== [32000] Application Header, Response
FIR(1) FIN(1) CON(0) UNS(0) SEQ# 3 IIN(0x0000)

9.2 AGA12 Encryption Diagnostics

Extensive diagnostics are provided by the SCADAPack E RTU for AGA12 Encryption operation and communication.

- ***Diagnostic Filtering*** 77
- ***Routing Rule Diagnostics*** 78
- ***Diagnostic Example - Session Open Transactions*** 82
- ***Diagnostic Example - Session Re-establishment Transactions*** 89
- ***System Points*** 91

9.2.1 Diagnostic Filtering

A Command line diagnostic interface is provided on the SCADAPack E RTU for AGA12. For more information on command line operation and diagnostics, refer to the *SCADAPack E Operational Reference Manual*.

Set AGA12 Diag Filters.

Usage: AGA12DIAG mode filter [filter...]
Where: mode = ENABLE DISABLE
Where: filter = * SCM PACKET TRANSPORT LINK BYTES INROUTE OUTROUTE RAWBYTES TIMESTAMP

The filters can be set for various levels of diagnostics on AGA12 communications. See Diagnostic Example - Session Open Transactions 82 and Diagnostic Example - Session Re-establishment Transactions 89 for typical diagnostic output.

FILTER:

*	diagnostics - A large volume of information provided for each transaction
SCM	SCADA Cryptographic Module (highest AGA12 layer diagnostics)
PACKET	AGA12 packet receive header diagnostics
TRANSPORT	AGA12 transport (wrapper) diagnostics
LINK	AGA12 link layer (receive and send length) diagnostics
BYTES	The data content bytes as each is decoded or built for each of the AGA12-2 processing layers
INROUTE	Inbound routing rule diagnostics
OUTROUTE	Outbound routing rule diagnostics
RAWBYTES	AGA12 frame bytes as they are received and transmitted on the communications port

9.2.2 Routing Rule Diagnostics

AGA12 & DNP3 Routing Diagnostics

Inbound AGA12 frames received on a cipertext port and not destined for the receiving node are routed according to DNP3 routing entries. They are routed and are not subject to the AGA12 processing rules or DNP3 routing rules that result is the diagnostic messages described in the following tables.

AGA12 frames destined for the receiving node are subject to routing rules and will produce messages described in the following tables.

DNP3 frames (being unsecured) are subject to routing rules and will produce messages described in the following tables.

SCADAPack E routing diagnostics refer to the route rule numbers.These are shown along with a description of their meaning in the following tables.

- ***Routing Rule Diagnostics for Inbound DNP3 Frames*** 78
- ***Routing Rule Diagnostics for Inbound AGA12 Frames*** 79
- ***Routing Rule Diagnostics for Unsolicited, Peer, Master Messages*** 80

Routing Rule Diagnostics for Inbound DNP3 Frames

When the AGADIAG ENABLE INROUTE command is used, diagnostics similar to the following are shown referencing routing rules.

```
   AGA12>>Inbound DNP3 frame from 32002. Process Frame for Me (Rule
D9)
```

The routing rule numbers have the following meanings:

Rule	Meaning
D1	Security is not enabled, DNP3 message is for me and is processed
D2	Security is not enabled, DNP3 message has a route in the route table and is routed in Clear Text
D3	DNP3 Clear Text message is received for me on a Cipher Text port in Mixed Mode (not as a Data Concentrator). Message is discarded
D4	DNP3 Clear Text message is received on a Cipher Text port in Mixed Mode. A route entry has no Security Level so is routed in Clear Text
D5	DNP3 Clear Text message is received on a Cipher Text port in Mixed Mode. A route entry has AGA12 security level, so message is discarded
D6	DNP3 message is received on Local Access port for me, and is processed
D7	DNP3 message is received by a AGA12 Gateway in Mixed Mode on the Local Access port. A route entry has no security level and is routed in Clear Text
D8	DNP3 Clear Text message is received by a AGA12 Gateway on a Local Access port in Mixed Mode. A route entry has AGA12 security level, so message is discarded
D9	DNP3 message is received for me as a AGA12 Gateway on a Clear Text port, and is processed
D10	DNP3 message is received by a AGA12 Gateway in Mixed Mode on a Clear Text port. A route entry has no security level and is routed in Clear Text
D11	DNP3 message is received by a AGA12 Gateway in Mixed Mode on a Clear Text port. A

	route entry has AGA12 security level and is sent encrypted on a Cipher Text port
D12	DNP3 message is received by a AGA12 Gateway in Mixed Mode on a Clear Text port. A route entry has AGA12 security level but can't be sent to the Local Access port. Message is discarded
D13	DNP3 message is received by a AGA12 Gateway in Mixed Mode on a Clear Text port. A route entry has AGA12 security level but can't be sent to a Clear Text port. Message is discarded
D14	DNP3 Clear Text message is received on a Cipher Text port. Mixed mode is disabled so message is discarded
D15	DNP3 Clear Text message is received by a AGA12 Gateway on a Clear Text port. Mixed Mode is disabled,and even though a route entry has no security level, message is discarded
D16	DNP3 message is received by a AGA12 Gateway on a Clear Text port. A route entry has AGA12 security level and is sent encrypted on a Cipher Text port
D17	DNP3 message is received by a AGA12 Gateway on a Clear Text port. A route entry has AGA12 security level but can't be sent to the Local Access port. Message is discarded
D18	DNP3 message is received by a AGA12 Gateway on a Clear Text port. A route entry has AGA12 security level but can't be sent to a Clear Text port. Message is discarded
D19	DNP3 Clear Text message is received on a Local Access port. Mixed mode is disabled so message is discarded
D20	DNP3 message is received in Mixed Mode on the Local Access port. A route entry has no security level and is routed in Clear Text
D21	DNP3 Clear Text message is received on a Local Access port in Mixed Mode. A route entry has AGA12 security level, so message is discarded
D22	DNP3 Clear Text message from a slave device is received for me on a Cipher Text port, as a data concentrator in Mixed Mode, and is processed

Routing Rule Diagnostics for Inbound AGA12 Messages

When the AGADIAG ENABLE INROUTE command is used, diagnostics similar to the following are shown referencing routing rules.

```
AGA12>>Inbound AGA12 frame from 2 to 32002. Msg Sent in Clear Text (Rule A3)
```

The routing rule numbers have the following meanings:

Rule	Meaning
A1	Security is not enabled. AGA12 message from DNP3 port is discarded
A2	AGA12 message from CipherText port is for me and will be processed
A3	AGA12 message from CipherText port is routed (in ClearText) by AGA12 Gateway to ClearText port
A4	AGA12 message on CipherText port to other CipherText port has no route entry security level and is discarded
A5	AGA12 message on CipherText port cannot route to Local Access port, has no route entry security level, and is discarded
A6	AGA12 message on CipherText port is routed to other CipherText port

A7	AGA12 message on CipherText port cannot route to Local Access port, even though it has a route entry security level, and is discarded
A8	AGA12 message from CipherText port is routed (encrypted) by AGA12 Gateway to ClearText port
A9	AGA12 message fromLocal Access port cannot be routed and is discarded
A10	AGA12 message from ClearText port on AGA12 Gateway is for me and will be processed
A11	AGA12 message from ClearText port on AGA12 Gateway has a route entry Security Level and is routed (encrypted)
A12	AGA12 message from ClearText port on AGA12 Gateway has no route entry Security Level and is routed to ClearText port
A13	AGA12 message from ClearText port on AGA12 Gateway has no route entry Security Level, can't be routed to CipherText port, so is discarded
A14	AGA12 message from ClearText port on AGA12 Gateway has no route entry Security Level, can't be routed to Local Access port, so is discarded

Routing Rule Diagnostics for Unsolicited, Peer, Master Messages

When the AGADIAG ENABLE OUTROUTE command is used, diagnostics similar to the following are shown referencing routing rules.

```
AGA12>>Outbound Message to 30000. Msg Sent Encrypted (Rule O12)
```

The routing rule numbers have the following meanings:

Rule	Meaning
O1	Security is disabled. DNP3 message sent in Clear Text
O2	AGA12 Gateway in Mixed Mode. DNP3 message sent in Clear Text on a Clear Text port
O3	AGA12 Gateway in Mixed Mode. Slave RTU DNP3 message can't be sent on a Cipher Text port with route entry that has no security level. Message discarded
O4	AGA12 Gateway in Mixed Mode. DNP3 message sent as encrypted AGA12 message on a Cipher Text port.
O5	AGA12 Gateway in Mixed Mode. DNP3 message sent as encrypted AGA12 message on a Clear Text port.
O6	AGA12 Gateway, Mixed Mode disabled. The Route entry has no security level. DNP3 message is sent in Clear Text on a Clear Text port
O7	AGA12 Gateway, Mixed Mode disabled. DNP3 message sent as encrypted AGA12 message on a Clear Text port.
O8	AGA12 Gateway, Mixed Mode disabled. DNP3 message can't be sent on a Cipher Text port with route entry that has no security level. Message discarded
O9	AGA12 Gateway, Mixed Mode disabled. DNP3 message sent as encrypted AGA12 message on a Cipher Text port
O10	DNP3 message sent in Clear Text on Local Access port
O11	Mixed mode disabled. DNP3 message can't be sent on a Cipher Text port with route entry that has no security level. Message discarded
O12	DNP3 message sent as encrypted AGA12 message on a Cipher Text port

O13	Mixed mode enabled. DNP3 message sent to Slave RTU in Clear Text on a Cipher Text port as route entry has no security level
O14	Mixed mode enabled. DNP3 message can't be sent on a Cipher Text port with route entry that has no security level. Message discarded
O15	AGA12 Gateway in Mixed mode. DNP3 message sent to Slave RTU in Clear Text on a Cipher Text port as route entry has no security level

9.2.3 Diagnostic Example - Session Open Transactions

AGA12 Session Open Transactions:

AGA12DIAG ENABLE *

15:04:09.359

AGA12>>Bytes Rx on Port 0: 10 11 21 00 02 00 04 01 83 32 8F 8F 29 14 8C 07
AGA12>>Bytes Rx on Port 0: 8A 88 C7 53 CC D0 7C F2 B8 1B F1 93 8D 57 6A 22
AGA12>>Bytes Rx on Port 0: 1A 43 25 75 B3 EA DA A4 A8 B4 F5 3D 6C D8 C4 65
AGA12>>Bytes Rx on Port 0: 71 B1 15 4E D0 58 08 D5 1A 87 DA 4E B5 A9 7B AF
AGA12>>Bytes Rx on Port 0: 7A CB D4 B8 8B F7 EF 8D E4 E6 AF 6D 21 0A 0B 9B
AGA12>>Bytes Rx on Port 0: F0 E0 B2 1E 2C DF 44 38 AC C7 CA BB 55 77 6D 3E
AGA12>>Bytes Rx on Port 0: 69 E0 10 15 CD 9E 8E 81 C4 6B 65 24 E9 83 3C 21
AGA12>>Bytes Rx on Port 0: 41 12 90 C1 CF 22 83 DC 72 AF 4A 1D 55 B3 4F B4
AGA12>>Bytes Rx on Port 0: C0 B4 45 26 CA 44 95 AE F7 F6 E0 8A 80 27 7F 8C
AGA12>>Bytes Rx on Port 0: E4 DF 9F F6 34 30 A0 F1 9C 57 0F AF DD 25 6C 07
AGA12>>Bytes Rx on Port 0: 4E BB DA 16 0E 1A E4 1A 91 73 93 0D EC 10 A6 0A
AGA12>>Bytes Rx on Port 0: D2 9E FC 10 15 83 1C E3 10 13 CC 4C 0E F6 7E 93
AGA12>>Bytes Rx on Port 0: 07 C9 E1 7B 71 37 C4 A8 9D CD F4 DE D8 AE 10 14

15:04:09.765

AGA12>>LinkLayer received packet: 200 bytes

21 00 02 00 04 01 83 32 8F 8F

29 14 8C 07 8A 88 C7 53 CC D0 7C F2 B8 1B F1 93
8D 57 6A 22 1A 43 25 75 B3 EA DA A4 A8 B4 F5 3D
6C D8 C4 65 71 B1 15 4E D0 58 08 D5 1A 87 DA 4E
B5 A9 7B AF 7A CB D4 B8 8B F7 EF 8D E4 E6 AF 6D
21 0A 0B 9B F0 E0 B2 1E 2C DF 44 38 AC C7 CA BB
55 77 6D 3E 69 E0 05 CD 9E 8E 81 C4 6B 65 24 E9
83 3C 21 41 12 90 C1 CF 22 83 DC 72 AF 4A 1D 55
B3 4F B4 C0 B4 45 26 CA 44 95 AE F7 F6 E0 8A 80
27 7F 8C E4 DF 9F F6 34 30 A0 F1 9C 57 0F AF DD
25 6C 07 4E BB DA 16 0E 1A E4 1A 91 73 93 0D EC
10 A6 0A D2 9E FC 05 83 1C E3

CC 4C 0E F6 7E 93 07 C9 E1 7B 71 37 C4 A8 9D CD
F4 DE D8 AE

15:04:09.781

AGA12>>Transport.receiveBegin

15:04:09.781
AGA12>>Transport.receiveHeader 10 bytes
15:04:09.781
AGA12>>Transport.receiveHeader dest=2 src=4 sessionId=1 sequence=2201128847 type=1
15:04:09.781
AGA12>>Transport.updateMac in receivePayload 10 bytes
15:04:09.796
AGA12>>Packet.receiveHeader dest=2 src=4 session=1 type=1 size=0
15:04:09.796
AGA12>>Transport.receivePayload length 1+169
15:04:09.796
AGA12>>Transport.receiveTrailer
15:04:09.796
AGA12>>Packet.receiveTrailer
15:04:09.796
AGA12>>SessionRequest: base=0 expiry=278
15:04:09.796
AGA12>>SessionRequest: base=45785 expiry=72000
15:04:09.796
AGA12>>SessionRequest: base=9785 expiry=72000
15:04:09.812
AGA12>>SCM received: OPN[4->2 (1) nonce=2813167e {data id=2 resolution=100000 tolerance=21 base=0 expiry=278 suite=1 macLength=20 key=2FAC98B13B2E68AD43B486CC6709D21E macKey=93541242DB11551B678CCB3752A6DA3C2FD8C569}]
15:04:09.812
AGA12>>SCM remove Session broadcast <- 4 id=1
15:04:09.812
AGA12>>SCM remove Session broadcast <- 4 id=2
15:04:09.812
AGA12>>New session 2<->4(2)
15:04:09.812
AGA12>>SCM add 2 <-> 4 id=2
15:04:09.812
AGA12>>SessionRequest: base=0 expiry=256
15:04:09.828
AGA12>>New session broadcast<->4(1)
15:04:09.828
AGA12>>SCM add broadcast <- 4 id=1
15:04:09.828
AGA12>>SessionRequest: base=45785 expiry=72000
15:04:09.828
AGA12>>New session broadcast<->4(2)

15:04:09.828

AGA12>>SCM add broadcast <- 4 id=2

15:04:09.828

AGA12>>SessionRequest: base=9785 expiry=72000

15:04:09.828

AGA12>>SCM sending ACK[2->4 (1) nonceOpn=2813167e nonceAck=915621b7 {data id=2 resolution=100000 tolerance=51 base=0 expiry=256 suite=1 macLength=20 key=2FAC98B13B2E68AD43B486CC6709D21E macKey=93541242DB11551B678CCB3752A6DA3C2FD8C569}]

15:04:09.843

AGA12>>Transport.sendHeader dest=4 src=2 session=1 type=2

15:04:09.843

AGA12>>LinkLayer send header 10 bytes

22 00 04 00 02 01 7C 7C 3E DB

15:04:09.843

AGA12>>LinkLayer send payload 174 bytes

3A AF 3F 39 E1 DE 11 9F BF 21 B5 E1 DB 1E D8 7C
35 CB BF 67 57 2B 5F 14 36 07 BC C6 C9 2E 3A 7B
2C 83 DC 74 E3 21 13 4E 04 94 B7 B7 B4 C1 86 66
8A 21 FA C3 B1 3D 6C 16 08 43 58 F4 20 5D 27 95
56 7A C0 DC D4 C7 53 D5 03 AA 89 04 BE CD C0 93
11 2C 44 8A CF D7 A9 6D 7F 82 CF 92 C3 20 05 78
23 16 8D AD C1 C5 13 52 16 97 A9 45 38 0F F6 3E
8E AD 5E AD C9 B0 E0 21 BC 70 16 49 25 DB 13 AD
B8 10 32 B1 BC 17 36 9C E0 72 F6 BD 83 AB 8E 7C
46 70 C0 FD 54 29 C5 83 F4 05 27 D1 E1 19 BE 9C
2B BE 65 46 E5 F1 EE A0 D3 A2 96 7D 9F C0

15:04:09.859

AGA12>>Transport.update sent a block of 174 bytes

15:04:09.875

AGA12>>Transport.doFinal in sendTrailer

15:04:09.875

AGA12>>Transport.sendPayload length 1+173

15:04:09.875

AGA12>>LinkLayer send trailer 20 bytes

71 D2 DE 39 88 CF 06 87 51 09 8E BF A6 21 36 51
BA FC A8 0D

15:04:10.312

AGA12>>Tx Bytes on Port 0:

10 11 22 00 04 00 02 01 7C 7C 3E DB 3A AF 3F 39
E1 DE 11 9F BF 21 B5 E1 DB 1E D8 7C 35 CB BF 67
57 2B 5F 14 36 07 BC C6 C9 2E 3A 7B 2C 83 DC 74
E3 21 13 4E 04 94 B7 B7 B4 C1 86 66 8A 21 FA C3
B1 3D 6C 16 08 43 58 F4 20 5D 27 95 56 7A C0 DC
D4 C7 53 D5 03 AA 89 04 BE CD C0 93 11 2C 44 8A
CF D7 A9 6D 7F 82 CF 92 C3 20 10 15 78 23 16 8D
AD C1 C5 13 52 16 97 A9 45 38 0F F6 3E 8E AD 5E
AD C9 B0 E0 21 BC 70 16 49 25 DB 13 AD B8 10 32
B1 BC 17 36 9C E0 72 F6 BD 83 AB 8E 7C 46 70 C0
FD 54 29 C5 83 F4 10 15 27 D1 E1 19 BE 9C 2B BE
65 46 E5 F1 EE A0 D3 A2 96 7D 9F C0 10 13 71 D2
DE 39 88 CF 06 87 51 09 8E BF A6 21 36 51 BA FC
A8 0D 10 14

AGA12 DNP3 Request / Response Transactions:

15:09:09.140

AGA12>>Bytes Rx on Port 0: 10 11 23 00 02 00 04 02 00 00 00 62 40 86 AD 5E
AGA12>>Bytes Rx on Port 0: 02 6E 3F 9E CB 74 85 BD 03 C3 5F A8 D3 AF 3F 47
AGA12>>Bytes Rx on Port 0: 39 24 2D CC E0 8F E9 6D 2C 53 F0 9E F8 B8 CA AA
AGA12>>Bytes Rx on Port 0: B9 29 69 64 8C 60 90 C2 1C 1C 67 CD C0 5F 4A 57
AGA12>>Bytes Rx on Port 0: C3 A8 FB E6 95 5C 07 E0 69 DC BF
AGA12>>Bytes Rx on Port 0: AF A4 BD AB AF 96 38 C0 7B 46 C6 19 86 DF FA CA
AGA12>>Bytes Rx on Port 0: AA DF 48 BD 86 51 66 3F 72 F4 C7 86 B2 6B 13 3B
AGA12>>Bytes Rx on Port 0: 90 90 73 7F 8F 26 9B AE 06 B9 53 04 86 35
AGA12>>Bytes Rx on Port 0: 10 13 C9 A2 2F 2B CC AC 28 C5 71 9D 9D E4 C2 8C
AGA12>>Bytes Rx on Port 0: C7 C2 CA 58 F9 1B 10 14

15:09:09.546

AGA12>>LinkLayer received packet: 139 bytes

23 00 02 00 04 02 00 00 00 62

40 86 AD 5E 02 6E 3F 9E CB 74 85 BD 03 C3 5F A8
D3 AF 3F 47 39 24 2D CC E0 8F E9 6D 2C 53 F0 9E
F8 B8 CA AA B9 29 69 64 8C 60 90 C2 1C 1C 67 CD
C0 5F 4A 57 C3 A8 FB E6 95 5C 07 E0 69 DC BF AF
A4 BD AB AF 96 38 C0 7B 46 C6 19 86 DF FA CA AA
DF 48 BD 86 51 66 3F 72 F4 C7 86 B2 6B 13 3B 90

```
        90 73 7F 8F 26 9B AE 06 B9 53 04 86 35

    C9 A2 2F 2B CC AC 28 C5 71 9D 9D E4 C2 8C C7 C2
        CA 58 F9 1B

15:09:09.562
AGA12>>Transport.receiveBegin
15:09:09.562
AGA12>>Transport.receiveHeader 10 bytes
15:09:09.562
AGA12>>Transport.receiveHeader dest=2 src=4 sessionId=2 sequence=98 type=3
15:09:09.562
AGA12>>seq=98 readSeq=30 now=103 diff=5 maxdiff=51
15:09:09.562
AGA12>>Transport.updateMac in receivePayload 10 bytes
15:09:09.562
AGA12>>Packet.receiveHeader dest=2 src=4 session=2 type=3 size=0
15:09:09.578
AGA12>>SCM received: DTA[4->2 (2)]
15:09:09.578
AGA12>>Transport.receivePayload length 1+108
15:09:09.578
AGA12>>Transport.receiveTrailer
15:09:09.578
AGA12>>Packet.receiveTrailer

15:09:09.578
...> ch00 00004.>00002  PRIMARY LINK HEADER - UNCONFIRMED USER DATA
                FCV:0 FCB:0 DIR:1 Length:092

15:09:09.593
Security Route>>Inbound Frame Route Result = TO_ME. Rule A3


15:09:09.593
***> ch00 00004*>00002 FRAME ADDRESSED TO ME

15:09:09.593
---> ch00 00004->00002  TRANSPORT HEADER - First:1  Final:1  Sequence:01

15:09:09.593
~~~> ch00 00004~>00002  APPLICATION HEADER - READ
```

First:1 Final:1 Confirm:0 Sequence:02

15:09:09.609
<~~~ ch00 00004<~00002 APPLICATION HEADER - RESPONSE TO REQUEST
First:1 Final:1 Confirm:0 Sequence:02 IIN:0x8020

15:09:09.609
<--- ch00 00004<-00002 TRANSPORT HEADER - First:1 Final:1 Sequence:06

15:09:09.609
<... ch00 00004<.00002 PRIMARY LINK HEADER - UNCONFIRMED USER DATA
FCV:0 FCB:0 DIR:0 Length:177
15:09:09.609
AGA12>>Received Scada message: dest=4, src=2
15:09:09.625
AGA12>>Transport.sendHeader dest=4 src=2 session=2 type=3
15:09:09.625
AGA12>>LinkLayer send header 10 bytes
23 00 04 00 02 02 00 00 00 67

15:09:09.625
AGA12>>LinkLayer send payload 204 bytes
34 90 13 3B 94 06 CC 85 42 00 74 34 E3 B2 27 82
42 19 70 C4 55 EE 83 1C C2 3C 30 D4 F8 53 35 E2
0E 9F 02 C5 4B BD 8A 2D 71 BA 6C B2 12 48 16 0A
C3 2D AA AA 92 15 4A 2E 17 4A E0 26 B8 0A D5 1E
1C A4 1B 66 77 71 94 13 24 F6 0D 30 EA 4E B8 13
97 14 F5 A5 D1 29 21 ED 8F 49 07 9E D9 93 BA 33
42 38 EA EF 25 C2 4E 87 BB 55 1D 4E 9C 0F 71 CE
7C E0 D3 C2 97 A2 76 70 29 7C 09 57 D6 58 D9 69
DB BB BA 86 1D 65 8A 79 2D 8D 3A D4 CA 34 2A 1A
DF F6 B7 11 98 8D 4E 30 A3 38 01 EC 4B 15 11 A5
63 B9 1C 37 61 1F 82 DC 74 1D 03 7F EC 69 D8 04
7B 1E D3 E6 D9 9A FA FA E6 AC FA 49 25 34 D2 02
89 D0 12 CF D8 7B D5 82 64 A1 FF 72

15:09:09.640
AGA12>>Transport.update sent a block of 204 bytes
15:09:09.640
AGA12>>SCM sent DTA payload
15:09:09.656
AGA12>>Transport.doFinal in sendTrailer

15:09:09.656
AGA12>>Transport.sendPayload length 1+203
15:09:09.656
AGA12>>LinkLayer send trailer 20 bytes
E7 74 67 21 FA 36 04 1A 50 8D 3D 63 EF 97 0D 01
C2 05 B9 87

15:09:10.156
AGA12>>Tx Bytes on Port 0:

10 11 23 00 04 00 02 02 00 00 00 67 34 90 13 3B
94 06 CC 85 42 00 74 34 E3 B2 27 82 42 19 70 C4
55 EE 83 1C C2 3C 30 D4 F8 53 35 E2 0E 9F 02 C5
4B BD 8A 2D 71 BA 6C B2 12 48 16 0A C3 2D AA AA
92 15 4A 2E 17 4A E0 26 B8 0A D5 1E 1C A4 1B 66
77 71 94 13 24 F6 0D 30 EA 4E B8 13 97 14 F5 A5
D1 29 21 ED 8F 49 07 9E D9 93 BA 33 42 38 EA EF
25 C2 4E 87 BB 55 1D 4E 9C 0F 71 CE 7C E0 D3 C2
97 A2 76 70 29 7C 09 57 D6 58 D9 69 DB BB BA 86
1D 65 8A 79 2D 8D 3A D4 CA 34 2A 1A DF F6 B7 11
98 8D 4E 30 A3 38 01 EC 4B 15 11 A5 63 B9 1C 37
61 1F 82 DC 74 1D 03 7F EC 69 D8 04 7B 1E D3 E6
D9 9A FA FA E6 AC FA 49 25 34 D2 02 89 D0 12 CF
D8 7B D5 82 64 A1 FF 72 10 13 E7 74 67 21 FA 36
04 1A 50 8D 3D 63 EF 97 0D 01 C2 10 15 B9 87 10
14

9.2.4 Diagnostic Example - Session Re-establishment Transactions

AGA12 Session Re-establishment Transactions:

... NEW SESSION REQUEST FROM REMOTE DEVICE IS RECEIVED HERE ...

17:37:39.165
AGA12>>SessionRequest: base=0 expiry=49
17:37:39.166
AGA12>>SCM received: OPN[20000->3 (1) nonce=f11ebf5e {data id=2 resolution=10000 0 tolerance=46 base=0 expiry=49 }]
17:37:39.166
AGA12>>New session 3<->20000(2)
17:37:39.167
AGA12>>SCM add 3 <-> 20000 id=2
17:37:39.167
AGA12>>SessionRequest: base=0 expiry=47
17:37:39.168
AGA12>>SCM sending ACK[3->20000 (1) nonceOpn=f11ebf5e nonceAck=feb7c6e0 {data id =2 resolution=100000 tolerance=46 base=0 expiry=47 }]
17:37:39.467
AGA12>>SCM received: DTA[20000->3 (2)]
17:37:39.475
AGA12>>Inbound AGA12 frame from 32000. Process Frame for Me (Rule A2)
17:37:39.481
AGA12>>Received Scada message: dest=20000, src=3
17:37:39.483
AGA12>>SCM sent DTA payload

... SESSION TIMES-OUT LOCALLY AND IS DISCONNECTED HERE ...

17:37:43.852
AGA12>>Session Timeout for ID 2
17:37:43.852
AGA12>>SCM sending: CLS[3->20000 (2)]
17:37:43.853
AGA12>>SCM remove Session 3 <-> 20000 id=2

... NEW SESSION REQUEST FROM REMOTE DEVICE IS RECEIVED HERE ...

17:37:46.811
AGA12>>SessionRequest: base=0 expiry=45
17:37:46.812
AGA12>>SCM received: OPN[20000->3 (1) nonce=c76c68fd {data id=2 resolution=10000 0 tolerance=46 base=0 expiry=45 }]
17:37:46.812
AGA12>>New session 3<->20000(2)
17:37:46.813
AGA12>>SCM add 3 <-> 20000 id=2
17:37:46.813
AGA12>>SessionRequest: base=0 expiry=41
17:37:46.814
AGA12>>SCM sending ACK[3->20000 (1) nonceOpn=c76c68fd nonceAck=ba60f068 {data id =2 resolution=100000 tolerance=46 base=0 expiry=41 }]
17:37:47.113
AGA12>>SCM received: DTA[20000->3 (2)]

17:37:47.122
AGA12>>Inbound AGA12 frame from 32000. Process Frame for Me (Rule A2)
17:37:47.127
AGA12>>Received Scada message: dest=20000, src=3
17:37:47.129
AGA12>>SCM sent DTA payload

... SESSION TIMES-OUT LOCALLY AND IS DISCONNECTED HERE ...
17:37:50.894
AGA12>>Session Timeout for ID 2
17:37:50.895
AGA12>>SCM sending: CLS[3->20000 (2)]
17:37:50.896
AGA12>>SCM remove Session 3 <-> 20000 id=2

9.2.5 System Points

The follow system points are provided for monitoring security status on the SCADAPack E RTU:

Security Information	System Point Address	Description
Security Mode	Analog Input 57600 (read only)	0=None 1=AGA12 RTU 2=AGA12 Gateway
AGA12 Mixed Mode	Binary Input 50740 (read/write)	Enabled / Disabled* * Only Disabled state can be written as per AGA12 rules

Communication Performance Monitoring

Performance Counter	System Point Address (Analog Input)	Description
AGA12 Open Failures	57610	Session negotiation rejections (e.g. not a configured or authorized SCM)
AGA12 HMAC Failures	57611	Frames where the verification signature doesn't match (e.g. content modified, frame corrupted, key mismatch)
AGA12 ACK Timeouts	57612	Session open attempts where no reply was received within the timeout period
AGA12 Frames Blocked	57613	AGA12 frames that couldn’t be delivered (e.g. no configured SCM address)
AGA12 Frames Routed	57614	Successfully routed AGA12 frames
AGA12 Frames Decoded	57615	Successful incoming frames correctly signed and decrypted
AGA12 Frames Encoded	57616	Outgoing frames successfully delivered

10 Attack Vectors & Requirements

The following descriptions are not for an exhaustive analysis of possible attack vectors, rather highlight usage guidelines (and reasons for those guidelines) when using DNP3 Secure Authentication and/or AGA12 on SCADAPack E RTUs. The intention is to make the user aware how to maximize the effectiveness of deploying security.

- ***Configurator or DNP3 to RTU & AGA 12 to RTU*** 93
- ***Routed Communication to RTU & Access to Gateway*** 95
- ***RTU Local Port Access, Networked Configurator, & Spoofing Master Address*** 96
- ***IP Networked RTU & Duplicated RTU Personality*** 97

10.1 Protocol and Configuration attacks on RTU

Configurator or DNP3 attack on RTU

The attacker uses SCADAPack E Configurator or other DNP3 software, through the SCADA comms link, to attempt to connect to RTU.

SCADAPack E Configurator uses DNP3 and operates in either clear text or using DNP3 Secure Authentication (if enabled). Similarly, an attack may attempt to utilize third party software with cleartext DNP3.

When DNP3 Secure Authentication is licensed and configured on the SCADAPack E RTU, the RTU challenges critical cleartext messages for itself. If a challenge reply is not forthcoming or is incorrect, the critical operation is not performed (e.g. control action, configuration change, etc).

When AGA12 security is licensed and configured, the RTU discards cleartext messages for itself (including wide area ports) other than local clear device port.

If the RTU is secured with DNP3 Secure Authentication, then the RTU may be protected using a default, common or unique security key. The RTU may optionally require the authentication information to include username / password credentials.

If the RTU is secured with AGA12, physical access is required to the local clear device port of the RTU. Remote access via DNP3 is only available through a gateway. External configuration messages to the RTU are protected. RTU needs to have matching key to the configuration in the gateway. User needs to have physical or network access to the secured gateway.

The RTU can optionally allow SCADAPack E Configurator software to change keys for maintenance flexibility. If so configured, it is highly recommended that DNP3 Secure Authentication also be enabled (so it challenges the writing and activation of the new security configuration).

Protocol Attacks on RTU

The attacker uses a security protocol mechanisms through the wide area network to attempt to connect to RTU.

If DNP3 Secure Authentication is licensed and configured, protocol attacks are repelled. Knowledge of the DNP3 security Update Key (Security Administrator Group's Common Key) is necessary for devices to correctly challenge and authenticate critical actions.

When using AGA12 communications, protocol attacks require the equivalent of an AGA12 Gateway, such as SCADAPack E RTU. This needs to be licensed and configured with Security and AGA12 Gateway options. Knowledge of both the encryption and hash keys is required for SCM configuration. The gateway node itself is protected by AGA12.

The AGA12 Gateway in a system needs to be installed in a physically and (networked) logically secure environment. Use of AGA12 Gateway in field installations is strongly discouraged.

Security Configuration Attacks on RTU

The attacker attempts to build a security configuration file to reconfigure the security settings of an RTU.

The SCADAPack E Security Administrator application utilizes a system master key inside the security configuration file. This master key is configured in SCADAPack E RTUs as a security administration function prior to controllers being installed in the field. Once set for this system, a security configuration generated by one system cannot be validly used on a different system.

Setting the Master Key on the Security Administrator application's PC and on each of the physical RTU devices is an important link in the security chain. This should be carried out by trusted personnel only.

10.2 Routed Communication to RTU & Access to Gateway

Routed Communication to RTU

The attacker routes across a wide area DNP3 SCADA network to attempt to connect to RTU.

DNP3 cleartext, DNP3 Secure Authentication and AGA12-2 SSPP cipher-text messages are routable by nodes, even when AGA12 is enabled.

The end node is responsible for protecting itself, as per ***Protocol and Configuration attacks on RTU*** 93.

Access to Gateway

An attacker attempts to connect to the AGA12 Gateway.

The Ethernet port on an AGA12 Gateway device is typically enabled for clear device operation, and DNP routing. Access from beyond the SCADA LAN is required to be protected by firewall. Physical access to the SCADA LAN would be required to compromise this. It is an important part of the security chain to protect physical access to the AGA12 Gateway.

An AGA12 Gateway will not answer cleartext requests on its ciphertext ports (even though it may route clear RTU responses back to the master station).

Remote access back in to the Gateway to read or disrupt routing requires AGA12 access and key knowledge. See ***Protocol Attacks on RTU*** 93.

Gateway security settings (and in fact security settings) are not exposed through remote links.

10.3 RTU Local Port Access, Networked Configurator & Spoofing Master Address

RTU Local Port Access

The attacker connects SCADAPack E Configurator or malicious software to AGA12 local clear device port on an RTU (at a site or a stolen device).

If AGA12 security is licensed and configured, but DNP3 Secure Authentication is not configured, the Local RTU may be compromised as physical access is available.

If DNP3 Secure Authentication is used, local configuration or control attempts will be challenged.

If RTU is operating with DNP3 Secure Authentication only, or in AGA12 Mixed Mode, messages may be routed throughout the network. Each RTU is responsible for its own protection. AGA12 protected RTUs will discard any cleartext messages from the network. DNP3 Secure Authentication configured devices will challenge any remote configuration or control attempts.

RTU device will not encrypt cleartext to AGA12 ciphertext.

Networked Configurator

An attacker sitting on a network behind the AGA12 Gateway uses SCADAPack E Configurator to attempt to connect to RTU.

The SCADA sub-network, where the authorized SCADAPack E Configurator is connected, requires IP security (e.g. firewall) to prevent unauthorized nodes from accessing the gateway.

If DNP3 Secure Authentication is licensed and configured, critical messages are challenged by the RTU.

Spoofing Master Address

An attacker spoofs the Master Station address to attempt to connect to RTU.

Scenarios are the same as described above for various connection points in the network. Requires either knowledge of Master address' encryption and hash keys, or requires physical access to RTUs. May also be possible through physical or logical access to SCADA LAN in order to access (and route through) the gateway. See ***Protocol Attacks on RTU*** 93 and ***Networked Configurator*** 96.

10.4 IP Networked RTUs & Duplicated RTU Personality

IP Networked RTUs

An attacker connects to the wide area IP network, attempting to connect to RTUs.

IP end-nodes, with DNP3 Secure Authentication enabled, process transported DNP3 frames as if they were arriving locally. They are treated the same way, so attack vectors described above apply, with respect to DNP3 data.

IP end-nodes, with AGA12 security enabled, process transported DNP3 frames as if they were arriving on a standard serial link. AGA12 encrypted DNP3 frames are treated the same way, so attack vectors described above apply, with respect to DNP3 data.

Remote DNP3 master station or configuration messages arriving at the RTU require either DNP3 Secure Authentication or AGA12 Encryption security, via an AGA12 Gateway.

IP security for access to IP device connectivity is not used by SCADAPack E RTUs.

Duplicated RTU Personality

An attacker takes a configuration file, or plug-in media and loads it on a stolen RTU

Security information is not included in standard RTU configurations that can be uploaded from an RTU. Duplicating the security personality of a protected RTU requires physical access to ‘security key’ media, possession of an authorized copy of the SCADAPack E Security Administrator software or knowledge of the keys used in the system.

An intercepted configuration file for a secured RTU cannot be validly loaded on an RTU unless the RTU has been set with an identical master key (requiring an original master key file as well). It is necessary to keep original master key files secured).

Security file information is itself encrypted and signed for tamper detection. Contents of a security file cannot be altered and re-used.

11 Using AGA12 Security Components - Copyright

AGA12 components in the SCADAPack E RTU firmware are based on reference code distributed under two public software licenses as detailed below.

The text of these licenses are reproduced here in accordance with requirements described in the AGA12 reference source code copyright notices and at http://scadasafe.sourceforge.net/LICENSE.

License for Cisco/AGA 12-1 Reference Implementation

The license applies to all software incorporated in the "Cisco/AGA 12-1 Reference Implementation" except for those portions incorporating third party software specifically identified as being licensed under separate license.

The Cisco Systems Public Software License, Version 1.0

Copyright (c) 2000 Cisco Systems, Inc. All rights reserved.

Subject to the following terms and conditions, Cisco Systems, Inc., hereby grants you a worldwide, royalty-free, nonexclusive, license, subject to third party intellectual property claims, to create derivative works of the Licensed Code and to reproduce, display, perform, sublicense, distribute such Licensed Code and derivative works. All rights not expressly granted herein are reserved.

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names Cisco and "Cisco/AGA 12-1 Reference Implementation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact opensource@cisco.com
4. Products derived from this software may not be called "Cisco" or "Cisco/AGA", nor may "Cisco" or "Cisco/AGA" appear in their name, without prior written permission of Cisco Systems, Inc.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL CISCO SYSTEMS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO

LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THAT EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU. FURTHER, YOU AGREE THAT IN NO EVENT WILL CISCO'S LIABILITY UNDER OR RELATED TO THIS AGREEMENT EXCEED AMOUNT FIVE THOUSAND DOLLARS (US) (US$5,000).

LICENSE TERMS

Copyright (c) 2002, Dr Brian Gladman, Worcester, UK. All rights reserved.

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.